ADSL Barricade

Broadband Router with built-in ADSL Modem

- Compatible with all leading DSLAMs
- Firewall (hacker attack logging, DoS, and client filtering)
- Supports DMT line modulation
- Four auto-negotiating 10/100 Ethernet ports
- Built-in print server
- PPTP, L2TP, and IPSec pass through
- Multiple user Internet access with a single user account
- Supports PPPoE and PPPoA
- Plug & Play installation
- Web-based management

SMC® Networks

User Guide

SMC7404BRA EU

Broadband Router with built-in ADSL Modem

From SMC's line of award-winning connectivity solutions

SMC® Networks

December 2002
Part No: 750.9701, UK 750.9735
Pub No: 150000035400A

COMPLIANCES

FCC - Class B

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with instructions, may cause harmful interference to radio communications. However, there is no guarantee that the interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

Note: In order to maintain compliance with the limits for a Class B digital device, you are required to use a quality interface cable when connecting to this device. Changes or modifications not expressly approved by our company could void the user's authority to operate this equipment.

FCC - Part 68

This equipment complies with Part 68 of the FCC rules. This equipment comes with a label attached to it that contains, among other information, the FCC registration number and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

This equipment uses the following USOC jacks: RJ-11C.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in the devices not ringing in response to an incoming call. In most, but not all areas, the sum of the RENs should not exceed five (5.0.) To be certain of the number of devices that may be connected to the line, as determined by the total RENs, contact the telephone company to determine the maximum REN for the calling area.

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. If advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations, or procedures that will provide advance notice in order for you to make the necessary

modifications in order to maintain uninterrupted service.

If trouble is experienced with this equipment, please contact our company at the numbers shown on back of this manual for repair and warranty information. If the trouble is causing harm to the telephone network, the telephone company may request you to remove the equipment from the network until the problem is resolved.

No repairs may be done by the customer.

This equipment cannot be used on telephone company-provided coin service. Connection to Party Line Service is subject to state tariffs.

When programming and/or making test calls to emergency numbers:

- Remain on the line and briefly explain to the dispatcher the reason for the call.
- Perform such activities in off-peak hours such as early morning or late evenings.

The Telephone Consumer Protection Act of 1991 makes it unlawful for any person to use a computer or other electronic device to send any message via a telephone facsimile machine unless such message clearly contains, in a margin at the top or bottom of each transmitted page or on the first page of the transmission the date and time it is sent and an identification of the business, other entity, or individual sending the message and the telephone number of the sending machine or such business, other entity, or individual.

In order to program this information into your facsimile, refer to your communications software user manual.

Industry Canada - Class B

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of Industry Canada.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le matérial brouilleur: "Appareils Numériques," NMB-003 édictée par l'Industrie.

Australia AS/NZS 3548 (1995) - Class B

EC Conformance Declaration - Class B

This information technology equipment complies with the requirements of the Council Directive 89/336/EEC on the Approximation of the laws of the Member States relating to Electromagnetic Compatibility and 73/23/EEC for electrical equipment used within certain voltage limits and the Amendment Directive 93/68/EEC. For the evaluation of the compliance with these Directives, the following standards were applied:

RFI Emission:
- Limit class B according to EN 55022:1998
- Limit class B for harmonic current emission according to EN 61000-3-2/1995
- Limitation of voltage fluctuation and flicker in low-voltage supply system according to EN 61000-3-3/1995

Immunity:
- Product family standard according to EN 55024:1998
- Electrostatic Discharge according to EN 61000-4-2:1995 (Contact Discharge: ±4 kV, Air Discharge: ±8 kV)
- Radio-frequency electromagnetic field according to EN 61000-4-3:1996 (80 - 1000 MHz with 1 kHz AM 80% Modulation: 3 V/m)
- Electrical fast transient/burst according to EN 61000-4-4:1995 (AC/DC power supply: ±1 kV, Data/Signal lines: ±0.5 kV)
- Surge immunity test according to EN 61000-4-5:1995 (AC/DC Line to Line: ±1 kV, AC/DC Line to Earth: ±2 kV)
- Immunity to conducted disturbances, Induced by radio-frequency fields: EN 61000-4-6:1996 (0.15 - 80 MHz with 1 kHz AM 80% Modulation: 3 V/m)
- Power frequency magnetic field immunity test according to EN 61000-4-8:1993 (1 A/m at frequency 50 Hz)
- Voltage dips, short interruptions and voltage variations immunity test according to EN 61000-4-11:1994 (>95% Reduction @10 ms, 30% Reduction @500 ms, >95% Reduction @5000 ms)

LVD:
- EN 60950 (A1/1992; A2/1993; A3/1993; A4/1995; A11/1997)

TABLE OF CONTENTS

1 Introduction 1-1

About the Barricade 1-1
Features and Benefits 1-1
Applications 1-3

2 Installation 2-1

Package Contents 2-1
System Requirements 2-2
Hardware Description 2-3
LEDs 2-4
Connect the System 2-5
Connect the ADSL Line 2-6
Phone Line Configuration 2-6
Connect the Power Adapter 2-8

3 Configuring Client PCs 3-1

TCP/IP Configuration 3-1

4 Configuring the Barricade 4-1

Navigating the Web Browser Interface 4-2
Making Configuration Changes 4-2
Setup Wizard 4-3
Time Zone 4-3
Internet Sharing 4-4
Parameter Setting 4-5
Finish 4-6
PPPoE & PPPoA 4-7
Finish 4-8
Multiple Protocol over ATM Mode 4-10
Finish 4-11
Advanced Setup 4-13
Navigating the Web Browser Interface 4-13
Making Configuration Changes 4-15
System Settings 4-16
Time Zone 4-16

Password Settings 4-17
Remote Management 4-18
DNS 4-19
WAN 4-20
PPPoE (PPP over Ethernet) 4-20
ATM 4-22
ISP 4-23
LAN 4-24
NAT 4-26
Address Mapping 4-27
Virtual Server 4-28
Routing System 4-30
Static Route 4-30
RIP 4-31
Routing Table 4-33
Firewall 4-34
Access Control 4-35
Access Control: Add PC 4-37
URL Blocking 4-38
Schedule Rule 4-39
Intrusion Detection 4-41
DMZ 4-46
SNMP 4-47
Community 4-47
Trap 4-48
ADSL 4-49
Parameters 4-49
Status 4-50
Tools 4-53
Configuration Tools 4-53
Firmware Upgrade 4-54
Reset 4-55
Status 4-56

5 Configuring Client TCP/IP 5-1

Windows 95/98/Me 5-1
Disable HTTP Proxy 5-4

Obtain IP Settings from Your ADSL Router 5-5
Windows NT 4.0 5-6
Disable HTTP Proxy 5-9
Obtain IP Settings from Your Barricade 5-9
Windows 2000 5-11
Disable HTTP Proxy 5-13
Obtain IP Settings from Your Barricade 5-13
Windows XP 5-15
Disable HTTP Proxy 5-17
Obtain IP Settings from Your Barricade 5-17
Configuring Your Macintosh Computer 5-19
Disable HTTP Proxy 5-21
Obtain IP Settings from Your Barricade 5-23

6 Configuring Printer Services 6-1

Install the Printer Port Monitor 6-1
Configure the Print Server 6-4
Configure the Network Printer in Windows 95/98/Me/2000 . 6-4
Configure the Network Printer in Windows NT 6-6
Configure the Network Printer in Unix Systems 6-7

A Troubleshooting A-1

B Cables B-1

Ethernet Cable B-1
Specifications B-1
Wiring Conventions B-1
RJ-45 Port Ethernet Connection B-2
Pin Assignments B-2
ADSL Cable Connection B-4
Specifications B-4
Wiring Conventions B-4

C Specifications C-1

CHAPTER 1
INTRODUCTION

Congratulations on your purchase of the Barricade Broadband Router with built-in ADSL Modem (SMC7404BRA EU.) We are proud to provide you with a powerful yet simple communication device for connecting your local area network (LAN) to the Internet. For those who want to surf the Internet in the most secure way, this Router provides a convenient and powerful solution.

About the Barricade

The Barricade provides Internet access to multiple users by sharing a single-user account. This new technology provides many secure and cost-effective functions. It is simple to configure and can be up and running in minutes.

Features and Benefits

- Internet connection via an RJ-11 WAN port.
- Local network connection via four 10/100 Mbps Ethernet ports.
- DHCP for dynamic IP configuration, and DNS for domain name mapping.
- Firewall with Stateful Packet Inspection, client privileges, intrusion detection, and NAT.

- NAT also enables multi-user Internet access via a single user account, and virtual server functionality (providing protected access to Internet services such as Web, FTP, e-mail, and Telnet.)
- VPN pass-through (IPSec-ESP Tunnel mode, L2TP, PPTP.)
- User-definable application sensing tunnel supports applications requiring multiple connections.
- Easy setup through a Web browser on any operating system that supports TCP/IP.
- Compatible with all popular Internet applications.

Applications

Many advanced networking features are provided by the Barricade:

- **Wired LAN**

  The Barricade provides connectivity to wired 10/100 Mbps devices, making it easy to create a network in small offices or homes.

- **Internet Access**

  This device supports Internet access through a DSL connection. Since many DSL providers use PPPoE or PPPoA to establish communications with end users, the Barricade includes built-in clients for these protocols, eliminating the need to install these services on your computer.

- **Shared IP Address**

  The Barricade provides Internet access for up to 253 users via a single shared IP address. Using only one ISP account, multiple users on your network can browse the Web at the same time.

- **Virtual Server**

  If you have a fixed IP address, you can set the Barricade to act as a virtual host for network address translation. Remote users access various services at your site using a constant IP address. Then, depending on the requested service (or port number), the Barricade can route the request to the appropriate server (at another internal IP address.) This secures your network from direct attack by hackers, and provides more flexible management by allowing you to change internal IP addresses without affecting outside access to your network.

- **DMZ Host Support**

  Allows a networked computer to be fully exposed to the Internet. This function is used when NAT and firewall security prevent an Internet application from functioning correctly.

- **Security**

  The Barricade supports security features that deny Internet access to specified users, or filter all requests for specific services the administrator does not want to serve. The Barricade's firewall also blocks common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding.

- **Virtual Private Network (VPN)**

  The Barricade supports three of the most commonly used VPN protocols – PPTP, L2TP, and IPSec. These protocols allow remote users to establish a secure connection to their corporate network. If your service provider supports VPNs, then these protocols can be used to create an authenticated and encrypted tunnel for passing secure data over the Internet (i.e., a traditionally shared data network.) The VPN protocols supported by the Barricade are briefly described below.

  - Point-to-Point Tunneling Protocol – Provides a secure tunnel for remote client access to a PPTP security gateway. PPTP includes provisions for call origination and flow control required by ISPs.
  - L2TP merges the best features of PPTP and L2F. Like PPTP, L2TP requires that the ISP's routers support the protocol.
  - IP Security – Provides IP network-layer encryption. IPSec can support large encryption networks (such as the Internet) by using digital certificates for device authentication.

CHAPTER 2
INSTALLATION

Before installing the Barricade Broadband Router with built-in ADSL Modem, verify that you have all the items listed under "Package Contents." If any of the items are missing or damaged, contact your local distributor. Also be sure that you have all the necessary cabling before installing the Barricade. After installing the Barricade, refer to "Configuring the Barricade" on page 4-1.

Package Contents

After unpacking the Barricade, check the contents of the box to be sure you have received the following components:

- Barricade ADSL Router (SMC7404BRA EU)
- Power adapter
- One CAT-5 Ethernet cable
- Telephone patch cable
- Documentation CD
- This User Guide
- ADSL service ordering guide

Immediately inform your dealer in the event of any incorrect, missing, or damaged parts. If possible, please retain the carton and original packing materials in case there is a need to return the product.

System Requirements

You must meet the following minimum requirements:

- Internet access from your Internet Service Provider (ISP) using a DSL modem.
- A PC using a fixed IP address or dynamic IP address assigned via DHCP, as well as a gateway server address and DNS server address from your service provider.
- A computer equipped with a 10 Mbps, 100 Mbps, or 10/100 Mbps Fast Ethernet card, or a USB-to-Ethernet converter.
- TCP/IP network protocols installed on each PC that will access the Internet.
- A Java-enabled Web browser, such as Microsoft Internet Explorer 4.0 or above or Netscape Communicator 4.0 or above installed on one PC at your site for configuring the Barricade.

Hardware Description

The Barricade contains an integrated DSL modem and connects to the Internet or to a remote site using its RJ-11 WAN port. It can be connected directly to your PC or to a local area network using any of the four RJ-45 Fast Ethernet LAN ports.

Access speed to the Internet depends on your service type. Full-rate ADSL provides up to 8 Mbps downstream and 640 kbps upstream. G.lite (or splitterless) ADSL provides up to 1.5 Mbps downstream and 512 Kbps upstream. However, you should note that the actual rate provided by specific service providers may vary dramatically from these upper limits.

Data passing between devices connected to your local area network can run at up to 100 Mbps over the Fast Ethernet ports.

The Barricade includes an LED display on the front panel for system power and port indications that simplifies installation and network troubleshooting. It also provides the following ports on the rear panel:

Item	Description
LAN Ports	Fast Ethernet ports (RJ-45.) Connect devices on your local area network to these ports (i.e., a PC, hub, or switch.)
Parallel printer port	One parallel printer port that can be connected to a printer. This printer can then be shared by all LAN users.
Reset Button	Use this button to reset the power and restore the default factory settings. To reset without losing configuration settings, see "Reset" on page 4-55.
Power Inlet	Connect the included power adapter to this inlet. **Warning**: Using the wrong type of power adapter may cause damage.
WAN Port	WAN port (RJ-11.) Connect your DSL line to this port.

LEDs

Verify Status

Check the power and port LED indicators.

LED	Condition	Status
Power	On	The Barricade is receiving power. Normal operation.
	Off	Power off or failure.
Ethernet (4 LEDs)	On	Ethernet Link.
	Flashing	Send/Receive data.
	Off	No Link.
ADSL Syn	On	ADSL connection is functioning correctly.
	Flashing	Startup.
	Off	ADSL connection is not established.
ADSL Data	Flashing	Send/Receive data.
	Off	No data transfering.

Connect the System

The Barricade can be positioned at any convenient location in your office or home. No special wiring or cooling requirements are needed. You should, however, comply with the following guidelines:

- Keep the Barricade away from any heating devices.
- Do not place the Barricade in a dusty or wet environment.

You should also remember to turn off the power, remove the power cord from the outlet, and keep your hands dry when you install the Barricade.

Connect the ADSL Line

Run standard telephone cable from the wall jack providing ADSL service to the WAN port on your Barricade. When inserting an ADSL RJ-11 plug, be sure the tab on the plug clicks into position to ensure that it is properly seated. If you are using splitterless ADSL service, be sure you add low-pass filters between the ADSL wall jack and your telephones. (These filters pass voice signals through but filter data signals out.)

Phone Line Configuration

Installing a Full-rate Connection

If you are using a full-rate (G.dmt) connection, your service provider will attach the outside ADSL line to a data/voice splitter. In this case you can connect your phones and computer directly to the splitter as shown below:

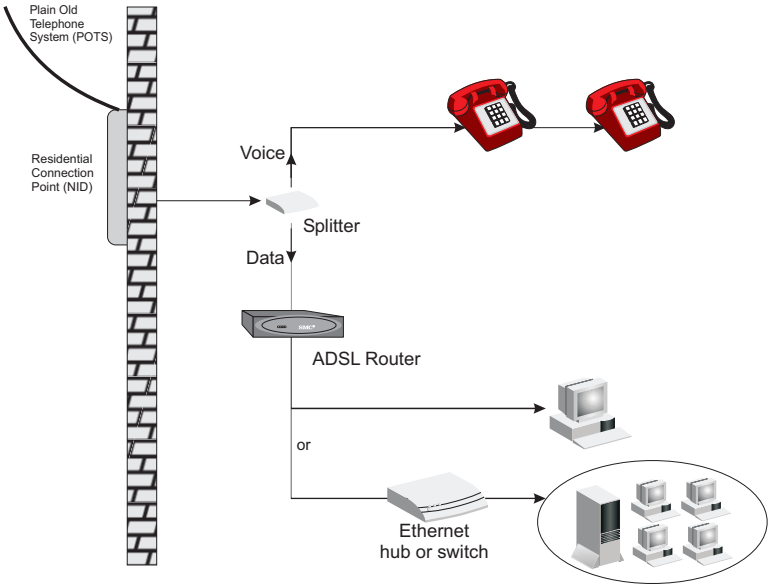


Figure 2-1. Installing With a Splitter

Installing a Splitterless Connection

If you are using a splitterless (G.lite) connection, then your service provider will attach the outside ADSL line directly to your phone system. In this case you can connect your phones and computer directly to the incoming ADSL line, but you will have to add low-pass filters to your phones as shown below:

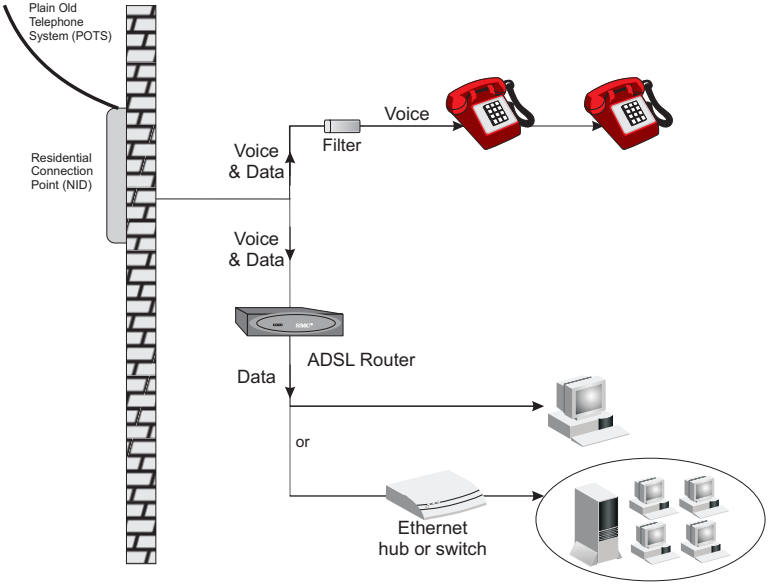


Figure 2-2. Installing Without a Splitter

Attach to Your Network Using Ethernet Cabling

The four LAN ports on the Barricade auto-negotiate the connection speed to 10 Mbps Ethernet or 100 Mbps Fast Ethernet, as well as the transmission mode to half-duplex or full-duplex.

Use twisted-pair cabling to connect any of the four LAN ports on the Barricade to an Ethernet adapter on your PC. Otherwise, cascade any of the LAN ports on the Barricade to an Ethernet hub or switch, and then connect your PC or other network equipment to the hub or switch. When

inserting an RJ-45 connector, be sure the tab on the connector clicks into position to ensure that it is properly seated.

Warning: Do not plug a phone jack connector into an RJ-45 port. This may damage the Barricade.

Notes: 1. Use 100-ohm shielded or unshielded twisted-pair cable with RJ-45 connectors for all Ethernet ports. Use Category 3, 4, or 5 for connections that operate at 10 Mbps, and Category 5 for connections that operate at 100 Mbps.

Notes: 2. Make sure each twisted-pair cable length does not exceed 100 meters (328 feet.)

Connect the Power Adapter

Plug the power adapter into the power socket on the rear of the Barricade, and the other end into a power outlet.

Check the power indicator on the front panel is lit. If the power indicator is not lit, refer to "Troubleshooting" on page A-1.

In case of a power input failure, the Barricade will automatically restart and begin to operate once the input power is restored.

If the Barricade is properly configured, it will take about 30 seconds to establish a connection with the ADSL service provider after powering up. During this time the Sync indicator will flash. After the ADSL connection has been established, the ADSL Sync LED will stay on.

CHAPTER 3
CONFIGURING CLIENT PCS

TCP/IP Configuration

To access the Internet through the Barricade, you must configure the network settings of the computers on your LAN to use the same IP subnet as the Barricade. The default network settings for the Barricade are:

IP Address: 192.168.2.1
Subnet Mask: 255.255.255.0

Note: These settings can be changed to fit your network requirements, but you must first configure at least one computer as described in "Configuring Client TCP/IP" on page 5-1 to access the Barricade's Web configuration interface in order to make the required changes. (See "Configuring the Barricade" on page 4-1 for instructions on configuring the Barricade.)

CHAPTER 4
CONFIGURING THE BARRICADE

After you have configured TCP/IP on a client computer, use a Web browser to configure the Barricade. The Barricade can be configured by any Java-supported browser including Internet Explorer 4.0 or above, or Netscape Navigator 4.0 or above. Using the Web management interface, you may configure the Barricade and view statistics to monitor network activity.

To access the Barricade's management interface, enter the IP address of the Barricade in your web browser:

http://192.168.2.1
(the Barricade automatically switches to Port 88 for management access.) Then click "LOGIN" (by default, there is no password.)

Note: For some browsers it may be necessary to include ":88" after the management IP address. For example, http://192.168.2.1:88

Navigating the Web Browser Interface

The Barricade's management interface consists of a Setup Wizard and an Advanced Setup section.

Setup Wizard: Use the Setup Wizard if you want to quickly setup the Barricade. Go to "Setup Wizard" on page 4-3.

Advanced Setup: Advanced Setup supports more advanced functions like hacker attack detection, IP and MAC address filtering, virtual server setup, virtual DMZ host, as well as other functions. Go to "Advanced Setup" on page 4-13.

Making Configuration Changes

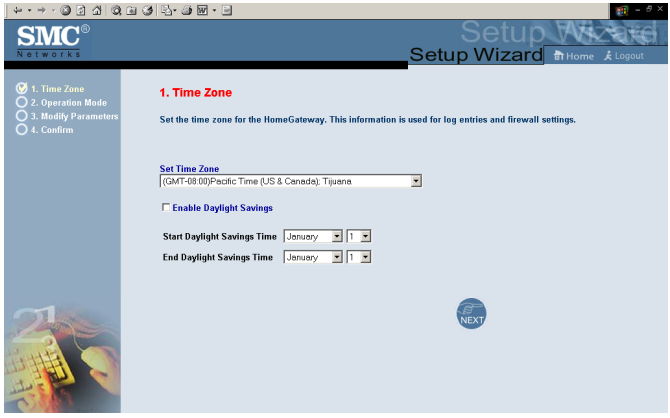
Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click the "Apply" or "Next" button at the bottom of the page to enable the new setting.

Note: To ensure proper screen refresh after a command entry, be sure that Internet Explorer 5.0 is configured as follows: Under the menu "Tools/Internet Options/General/Temporary Internet Files/Settings," the setting for "Check for newer versions of stored pages" should be "Every visit to the page."

Setup Wizard

Time Zone

Click on "Setup Wizard." The first item in the Setup Wizard is Time Zone setup.

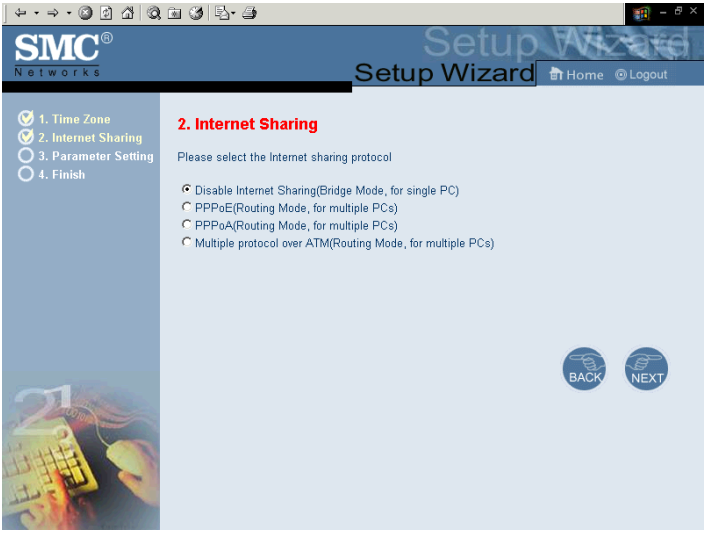


For accurate timing of log entries and system events, you need to set the time zone. Select your time zone from the dropdown list.

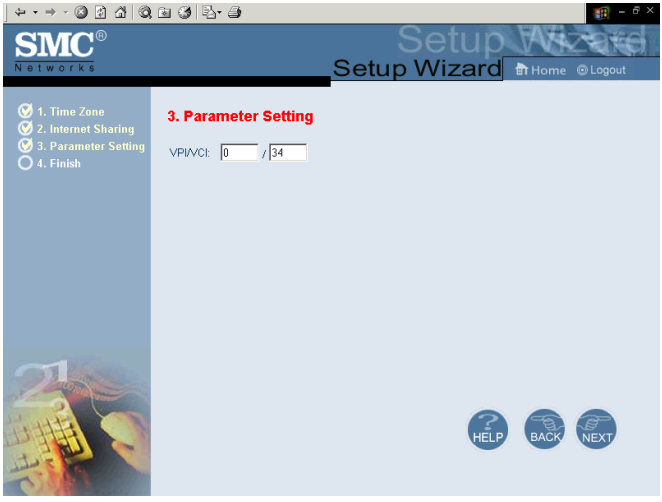
If your area requires it, check to enable the clock for daylight saving changes, and enter the Daylight Saving Time start and end dates for your location.

Internet Sharing

Select the operation mode. Go to "PPPoE & PPPoA" on page 4-7 if you will use either of these modes, and go to "Multiple Protocol over ATM Mode" on page 4-10 if you will use multiple protocol routing mode.

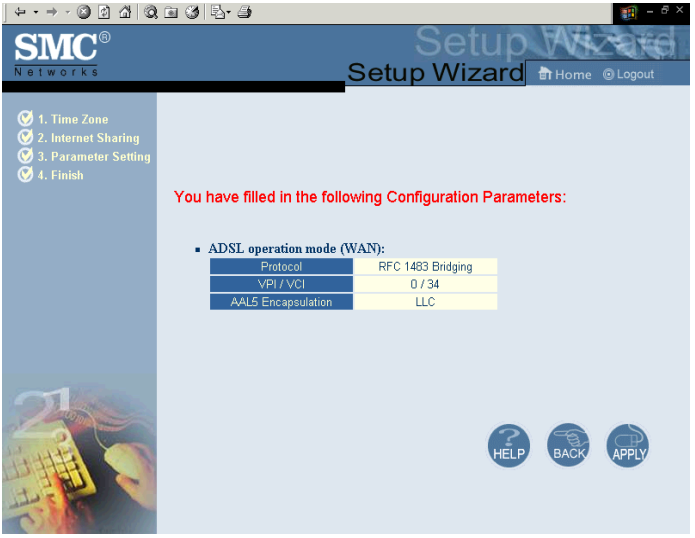


Parameter Setting



Parameter	Description
VPI/VCI	Data flows are broken up into fixed length cells, each of which contains a Virtual Path Identifier (VPI) that identifies the path between two nodes, and a Virtual Circuit Identifier (VCI) that identifies the data channel within that virtual path. Each virtual circuit maintains a constant flow of cells between the two end points. When there is no data to transmit, empty cells are sent. And when data needs to be transmitted, it is immediately inserted into the cell flows.

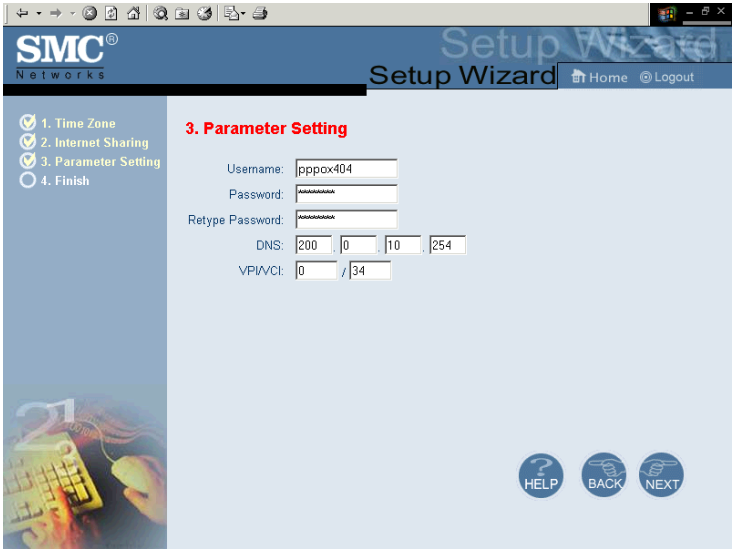
Finish



Parameter	Description
Protocol	Indicates the protocol used.
VPI/VCI	Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI.)
AAL5 Encapsulation	Shows the packet encapsulation type.

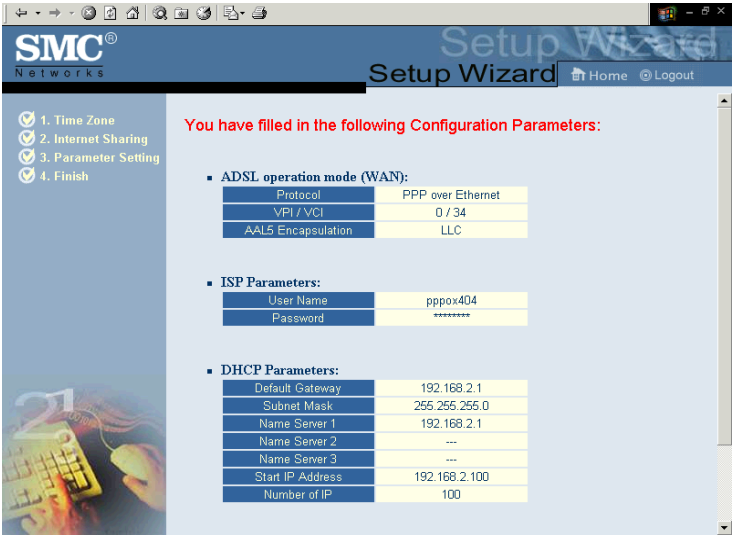
Your Barricade is now setup. Go to "Troubleshooting" on page A-1 if you cannot make a connection to the Internet.

PPPoE & PPPoA



Parameter	Description
Username	Enter the ISP assigned username.
Password	Enter your password.
Retype Password	Confirm the password.
DNS	Enter a domain name server IP address.
VPI/VCI	Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI.) Data flows are broken up into fixed length cells, each of which contains a Virtual Path Identifier (VPI) that identifies the path between two nodes, and a Virtual Circuit Identifier (VCI) that identifies the data channel within that virtual path. Each virtual circuit maintains a constant flow of cells between the two end points. When there is no data to transmit, empty cells are sent. And when data needs to be transmitted, it is immediately inserted into the cell flows.

Finish

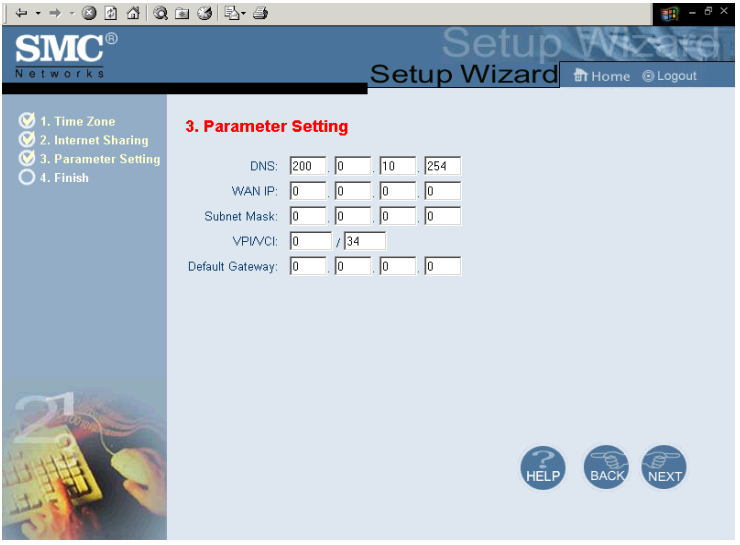


Parameter	Description
ADSL Operation Mode (WAN)	
Protocol	Indicates the protocol used
VPI/VCI	Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI.)
AAL5 Encapsulation	Shows the packet encapsulation type.
ISP Parameters	
Username	The ISP assigned username.
Password	The password (hidden.)

Parameter	Description
DHCP Parameters	
Default Gateway	The default gateway IP address. If the Barricade cannot find the destination address within its local network, it will forward the packets to the Default Gateway (usually your ISP will supply this address)
Subnet Mask	The network subnet mask.
Name Server 1	Primary name server IP address.
Name Server 2	Alternate name server IP address.
Name Server 3	Alternate name server IP address.
Start IP Address	Start IP Address of DHCP assigned IP addresses.
Number of IP	Number of IPs available for assignment by the DHCP server.

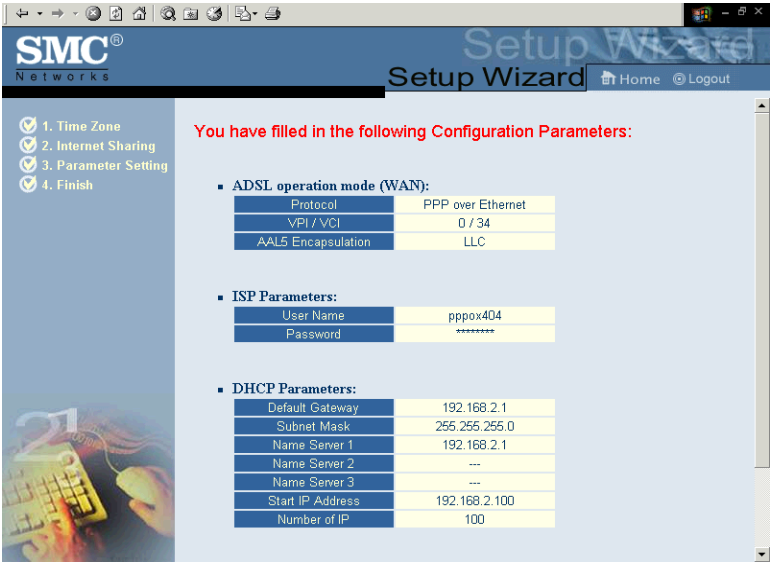
Your Barricade is now setup. Go to "Troubleshooting" on page A-1 if you cannot make a connection to the Internet.

Multiple Protocol over ATM Mode



Parameter	Description
DNS	Enter a domain name server IP address.
WAN IP	Enter an IP Address for the Barricade WAN interface.
Subnet Mask	Enter a subnet mask.
VPI/VCI	Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI.) Data flows are broken up into fixed length cells, each of which contains a Virtual Path Identifier (VPI) that identifies the path between two nodes, and a Virtual Circuit Identifier (VCI) that identifies the data channel within that virtual path. Each virtual circuit maintains a constant flow of cells between the two end points. When there is no data to transmit, empty cells are sent. And when data needs to be transmitted, it is immediately inserted into the cell flows.
Default Gateway	Enter a default gateway IP address. If the Barricade cannot find the destination address within its local network, it will forward the packets to the Default Gateway (usually your ISP will supply this address.)

Finish



Parameter	Description
ADSL Operation Mode (WAN)	
Protocol	Indicates the protocol used
VPI/VCI	Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI.)
AAL5 Encapsulation	Shows the packet encapsulation type.
Network Layer Parameters (WAN)	
IP Address	Shows the WAN IP address.
Subnet Mask	Shows the WAN Subnet Mask.
Default Gateway	Shows the WAN Default Gateway.

Parameter	Description
DHCP Parameters	
Default Gateway	The default gateway IP address. If the Barricade cannot find the destination address within its local network, it will forward the packets to the Default Gateway (usually your ISP will supply this address.)
Subnet Mask	The network subnet mask.
Name Server 1	Primary name server IP address.
Name Server 2	Alternate name server IP address.
Name Server 3	Alternate name server IP address.
Start IP Address	Start IP Address of DHCP assigned IP addresses.
Number of IP	Number of IPs available for assignment by the DHCP server.

Your Barricade is now setup. Go to "Troubleshooting" on page A-1 if you cannot make a connection to the Internet.

Advanced Setup

Clicking "Advanced Setup" displays the main menu on the left-hand side of the screen and descriptive information on the right-hand side. The Main Menu links are used to navigate to other menus that display configuration parameters and statistics.

Navigating the Web Browser Interface

The Barricade's advanced management interface contains ten main menu items – System, WAN, LAN, NAT, Routing system, Firewall, SNMP, ADSL, Tools, and Status.

The following table briefly describes the "Advanced Setup" menu items.

Menu	Description
System	Sets the local time zone, the password for administrator access, the IP address of a PC that will be allowed to manage the Barricade remotely, and the IP address of a domain name server.
WAN	Specifies the Internet connection settings.
LAN	Sets the TCP/IP configuration for the Barricade LAN interface and DHCP clients.
NAT	Shares a single ISP account with multiple users, sets up virtual servers.
Routing system	Sets routing parameters and displays the current routing table.
Firewall	Configures a variety of security and specialized functions including: Access Control, URL blocking, Internet access control scheduling, Intruder detection, and DMZ.
SNMP	Community string and trap server setting.
ADSL	Sets the ADSL operation type and shows the ADSL status.
Tools	Contains options to backup & restore the current configuration, restore all configuration settings to the factory defaults, update system firmware, or reset the system.
Status	Provides WAN connection type and status, firmware and hardware version numbers, system IP settings, as well as DHCP, NAT, Firewall info.
	Displays the number of attached clients, the firmware versions, the physical MAC address for each media interface, and the hardware version and serial number.
	Shows the security and DHCP client log.

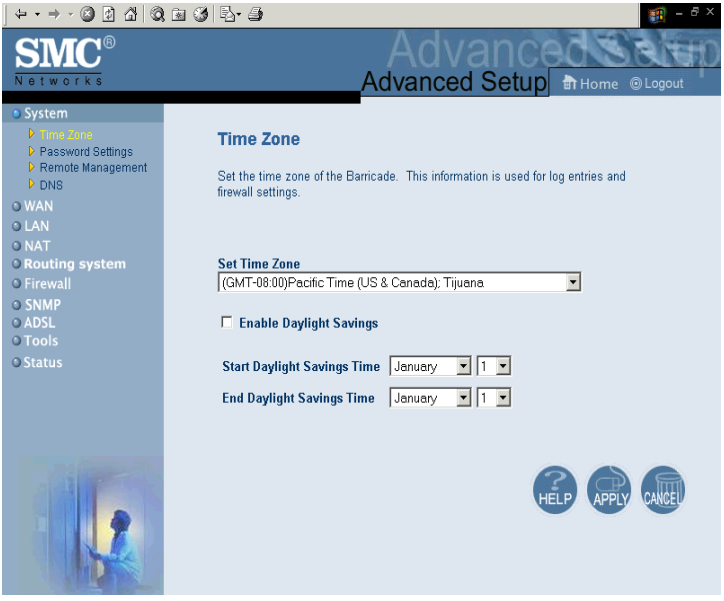
Making Configuration Changes

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click the "APPLY" or "NEXT" button at the bottom of the page to make the new settings active.

Note: To ensure proper screen refresh after a command entry, check that Internet Explorer 5.0 is configured as follows: Under the menu "Tools/Internet Options/General/Temporary Internet Files/ Settings," the setting for "Check for newer versions of stored pages" should be "Every visit to the page."

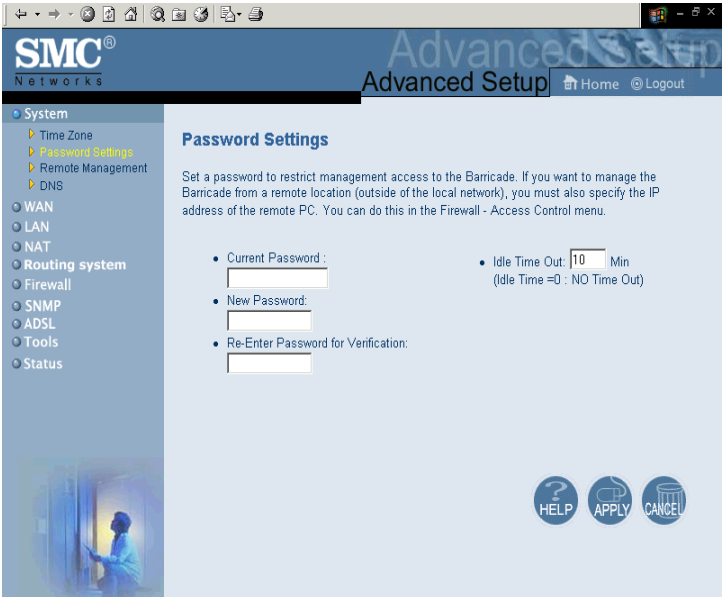
System Settings

Time Zone



Set your local time zone. This information is used for log entries and client filtering.

Password Settings

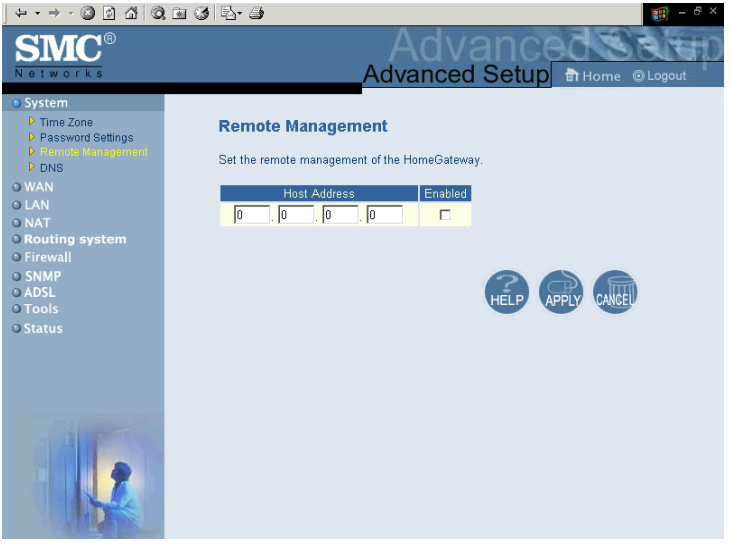


Use this page to restrict access based on a password. By default, there is no password. For security you should assign one before exposing the Barricade to the Internet.

Passwords can contain from 3–12 alphanumeric characters and are not case sensitive.

Note: If your password is lost, or you cannot gain access to the user interface, press the reset button (colored blue) on the rear panel (holding it down for at least five seconds) to restore the factory defaults. (Default is no password.)

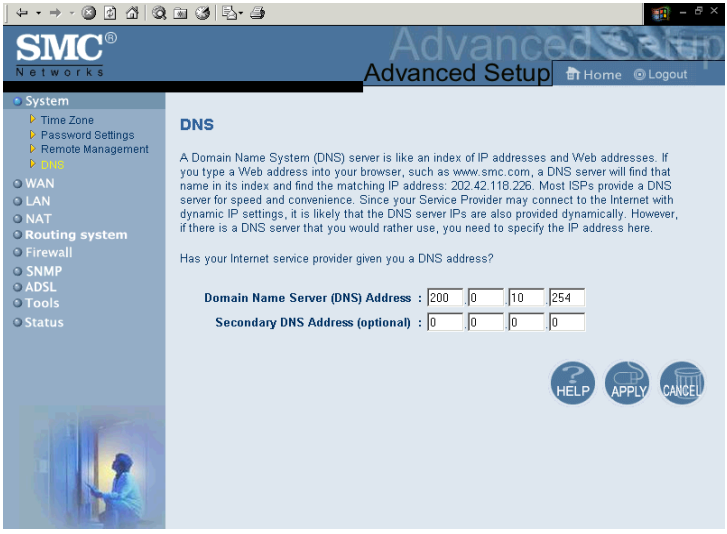
Remote Management



By default, management access is only available to users on your local network. However, you can also manage the Barricade from a remote host by entering the IP address of a remote computer on this screen. Check the "Enabled" box to enable this function.

Note: If you check "Enable" and specify an IP address of 0.0.0.0, any host can manage the Barricade.

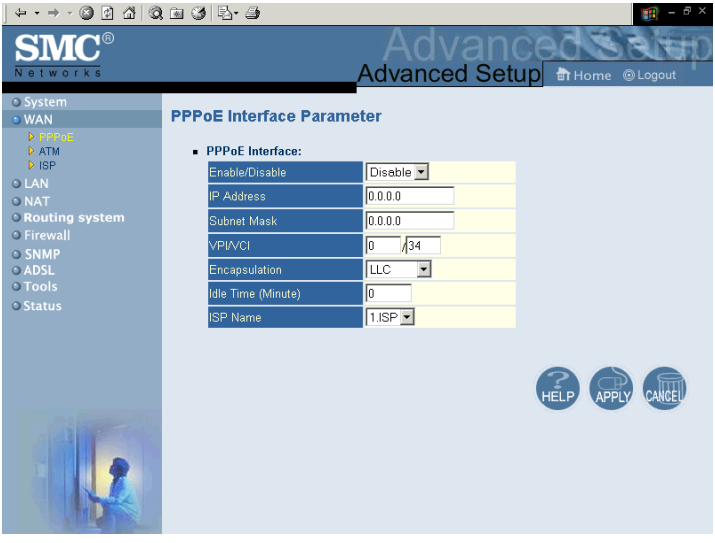
DNS


SMC Networks
Advanced Setup
Home
Logout
System
Time Zone
Password Settings
Remote Management
DNS
WAN
LAN
NAT
Routing system
Firewall
SNMP
ADSL
Tools
Status
DNS
A Domain Name System (DNS) server is like an index of IP addresses and Web addresses. If you type a Web address into your browser, such as www.smc.com, a DNS server will find that name in its index and find the matching IP address: 202.42.118.226. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect to the Internet with dynamic IP settings, it is likely that the DNS server IPs are also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP address here.
Has your Internet service provider given you a DNS address?
Domain Name Server (DNS) Address : 200 0 10 254
Secondary DNS Address (optional) : 0 0 0 0
HELP
APPLY
CANCEL

Domain Name Servers are used to map a domain name (e.g., www.smc.com) to the equivalent numerical IP address (e.g., 64.147.25.20.) Your ISP should provide the IP address of one or more domain name servers. Enter those addresses on this page.

WAN

PPPoE (PPP over Ethernet)



Parameter	Description
Enable/Disable	Enables/Disables the PPPoE Interface.
IP Address	If your IP address is assigned by the ISP each time you connect, leave this field all zeros. Otherwise, enter your ISP supplied static IP address here.
Subnet Mask	If your subnet mask is assigned by the ISP each time you connect, leave this field all zeros. Otherwise, enter your subnet mask here.

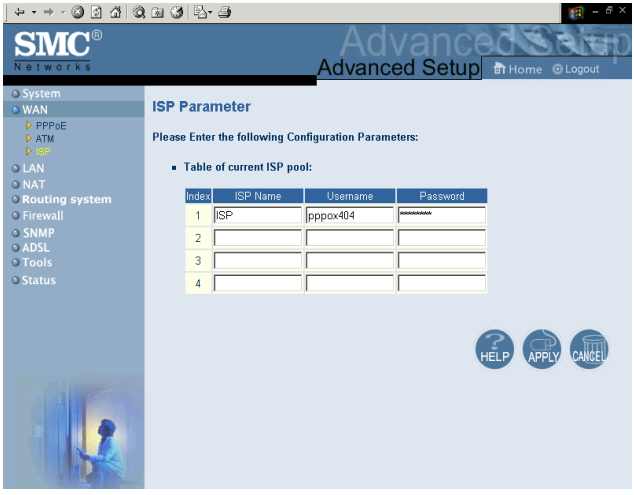
Parameter	Description
VPI/VCI	Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI.) Data flows are broken up into fixed length cells, each of which contains a Virtual Path Identifier (VPI) that identifies the path between two nodes, and a Virtual Circuit Identifier (VCI) that identifies the data channel within that virtual path. Each virtual circuit maintains a constant flow of cells between the two end points. When there is no data to transmit, empty cells are sent. When data needs to be transmitted, it is immediately inserted into the cell flows.
Encapsulation	Specifies how to handle multiple protocols at the ATM transport layer. • VC-MUX. Point to Point Protocol over ATM Virtual Circuit Multiplexer (null encapsulation) allows only one protocol running per virtual circuit with less overhead. • LLC. Point to Point Protocol over ATM Logical Link Control allows multiple protocols running over one virtual circuit (uses slightly more overhead.)
Idle Time (Minute)	Enter the maximum idle time for the Internet connection. After this time has been exceeded the connection will be terminated.
ISP Name	Choose the ISP to whom this connection will apply.

ATM

Parameter	Description
Protocol	• Disable: Disables the connection. • 1483 Bridging: Bridging is a standardized layer 2 technology. It is typically used in corporate networks to extend the physical reach of a single LAN segment and increase the number of stations on a LAN without compromising performance. Bridged data is encapsulated using the RFC1483 protocol to enable data transport. • PPPoA: Point-to-Point Protocol over ATM is a method of encapsulating data for transmission to a far point. • 1483 Routing: 1483 Routing allows a simple, low cost connection to the Internet via a standard 10BASE-T port. The router looks up the network address for each packet seen on the LAN port. If the address is listed in the routing table as local, it is filtered. If the address is listed under the ADSL port, it is forwarded. Or if the address is not found, then it is automatically forwarded to the default router (i.e., the ADSL router at the head end.)
IP Address	IP address of the ATM interface.
Subnet Mask	Subnet mask of the ATM interface.

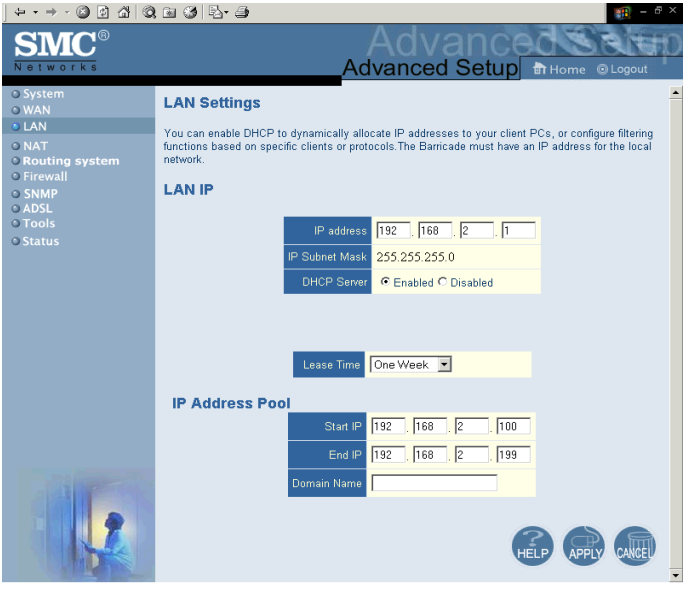
Parameter	Description
VPI/VCI	Virtual Path Indicator: Each connection must have a unique pair of VPI/VCI settings. Virtual Channel Indicator: Each connection must have a unique pair of VPI/VCI settings.
Encapsulation	Specifies how to handle multiple protocols at the ATM transport layer. • VC-MUX. Point to Point Protocol over ATM Virtual Circuit Multiplexer (null encapsulation) allows only one protocol running per virtual circuit with less overhead. • LLC. Point to Point Protocol over ATM Logical Link Control allows multiple protocols running over one virtual circuit with a little bit more overhead.

ISP



Enter the Internet Service Provider name, username, and password for each ISP connection you have.

LAN



Parameter	Description
LAN IP	
IP Address	The IP address of the Barricade.
IP Subnet Mask	Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI.)
DHCP Server	To dynamically assign an IP address to client PCs, enable the DHCP (Dynamic Host Configuration Protocol) Server.
Lease Time	Set the DHCP lease time.

Parameter	Description
IP Address Pool	
Start IP Address	Specify the start IP address of the DHCP pool. Do not include the gateway address of the Barricade in the client address pool. If you change the pool range, make sure the first three octets match the gateway's IP address, i.e., 192.168.2.xxx.
End IP Address	Specify the end IP address of the DHCP pool.
Domain Name	If your network uses a domain name, enter it here. otherwise leave this field blank

Remember to configure your client PCs for dynamic address allocation (See "Configuring Client PCs" on page 3-1 for details.)

NAT

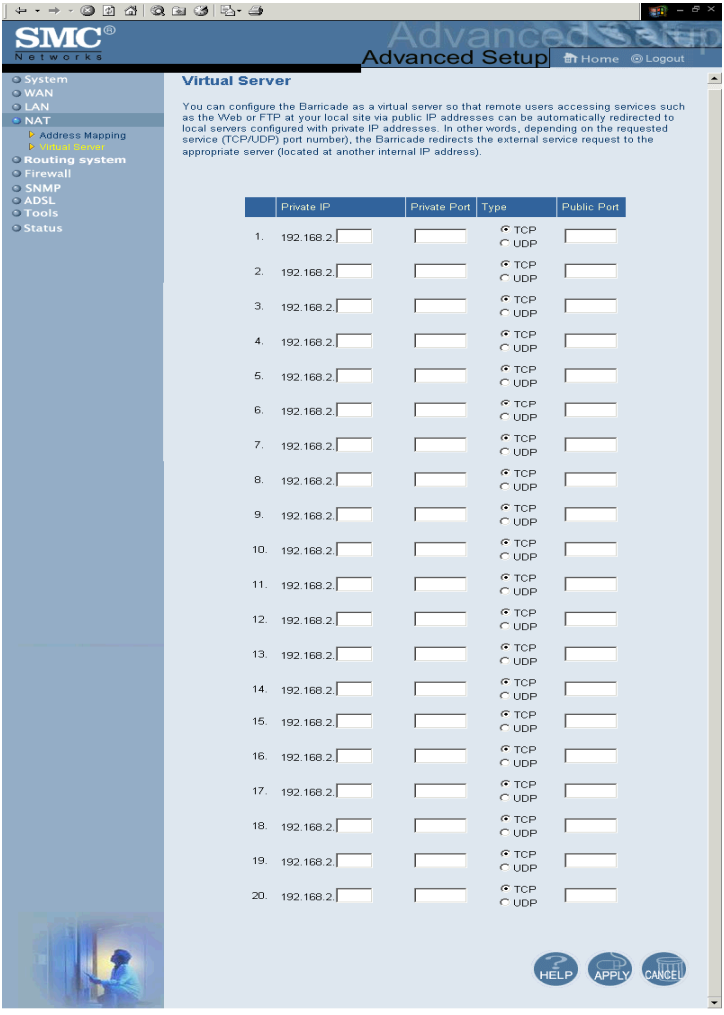
Some applications require multiple connections, such as Internet gaming, videoconferencing, Internet telephony, and others. These applications may not work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, use these pages to specify the additional public ports to be opened for each application.

Address Mapping

SMC Networks
Advanced Setup
Home
Logout
System
WAN
LAN
NAT
Address Mapping
Virtual Server
Routing system
Firewall
SNMP
ADSL
Tools
Status
Address Mapping
Network Address Translation (NAT) allows IP addresses used in a private local network to be mapped to one or more addresses used in the public, global Internet. This feature limits the number of public IP addresses required from the ISP and also maintains the privacy and security of the local network. We allow one or more than one public IP address to be mapped to a pool of local addresses.
Address Mapping
1. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 192.168.2. 0 to 192.168.2. 0
2. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 192.168.2. 0 to 192.168.2. 0
3. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 192.168.2. 0 to 192.168.2. 0
4. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 192.168.2. 0 to 192.168.2. 0
5. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 192.168.2. 0 to 192.168.2. 0
6. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 192.168.2. 0 to 192.168.2. 0
7. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 192.168.2. 0 to 192.168.2. 0
8. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 192.168.2. 0 to 192.168.2. 0
9. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 192.168.2. 0 to 192.168.2. 0
10. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 192.168.2. 0 to 192.168.2. 0
HELP
APPLY
CANCEL

Use "Address Mapping" to allow a limited number of public IP addresses to be translated into multiple private IP addresses for use on the internal LAN network. This also hides the internal network for increased privacy and security.

Virtual Server



If you configure the Barricade as a virtual server, remote users accessing services such as Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP

addresses. In other words, depending on the requested service (TCP/UDP port number), the Barricade redirects the external service request to the appropriate server (located at another internal IP address.)

For example, if you set Type/Public Port to TCP/80 (HTTP or Web) and the Private IP/Port to 192.168.2.2/80, then all HTTP requests from outside users will be transferred to 192.168.2.2 on port 80. Therefore, by just entering the IP Address provided by the ISP, Internet users can access the service they need at the local address to which you redirect them.

The more common TCP service ports include:

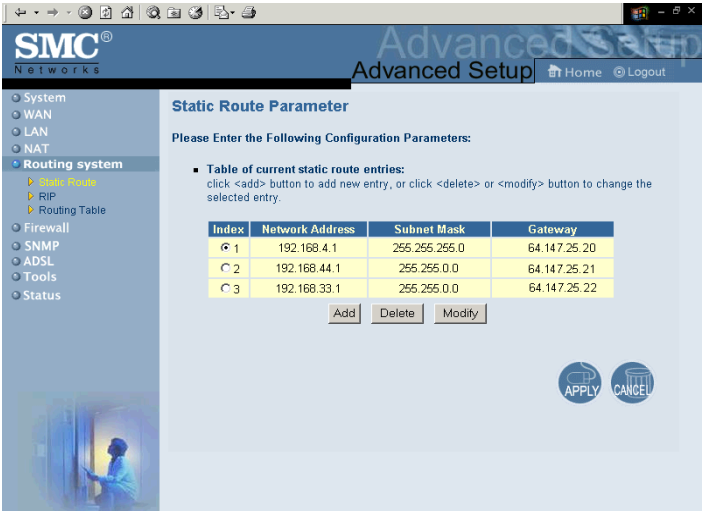
HTTP: 80, FTP: 21, Telnet: 23, and POP3: 110.

Note: The WAN interface should have a fixed IP address to best utilize this function. If your ISP only provides dynamic IP addresses, a search for "free dynamic IP" on any major search engine will turn up tools that will allow you to use the same domain name even though your IP address changes each time you log in to the ISP.

Routing System

These pages define routing related parameters, including static routes and RIP (Routing Information Protocol) parameters.

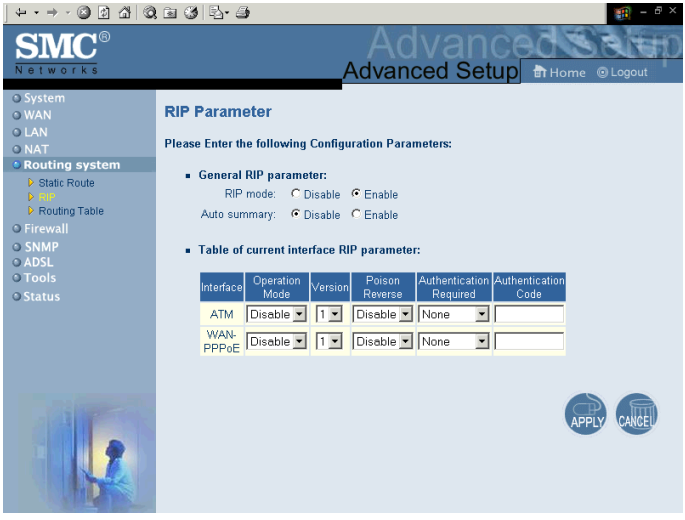
Static Route



Parameter	Description
Index	Check the box of the route you wish to delete or modify.
Network Address	Enter the IP address of the remote computer you wish to set a static route to.
Subnet Mask	Enter the subnet mask of the remote network you wish to set a static route to.
Gateway	Enter the WAN IP address of the gateway to the remote network.

Click "Add" to add a new static route to the list, or check the box of an already entered route and click "Modify." Clicking "Delete" will remove an entry from the list.

RIP

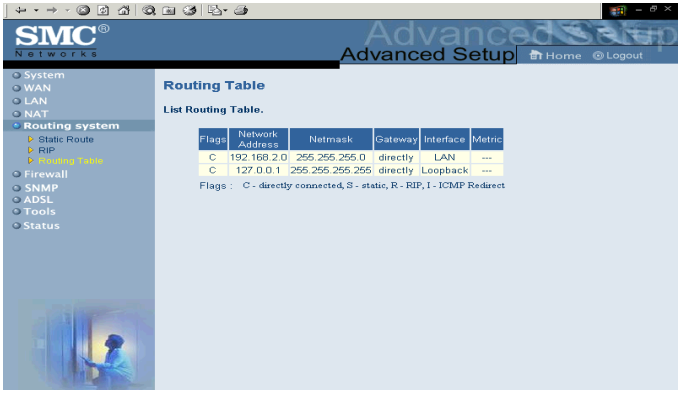


Parameter	Description
Interface	The WAN interface to be configured.
Operation Mode	Disable: RIP disabled on this interface. Enable: RIP enabled on this interface. Silent: Listens for route broadcasts and updates its route table. It does not participate in sending route broadcasts.
Version	Sets the RIP (Routing Information Protocol) version to use on this interface.
Poison Reverse	A poison reverse is a way in which a router tells its neighbor routers that one of the routers is no longer connected.

Parameter	Description
Authentication Required	• None: No authentication. • Password: A password authentication key is included in the packet. If this does not match what is expected, the packet will be discarded. This method provides very little security as it is possible to learn the authentication key by watching RIP packets. MD5: MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to a specific individual.
Authentication Code	Password or MD5 Authentication key.

RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. RIP routers maintain only the best route to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change.

Routing Table



Parameter	Description
Flags	Indicates the route status: C = Direct connection on the same subnet. S = Static route. R = RIP (Routing Information Protocol) assigned route. I = ICMP (Internet Control Message Protocol) Redirect route.
Network Address	Destination IP address.
Netmask	The subnetwork associated with the destination. This is a template that identifies the address bits in the destination address used for routing to specific subnets. Each bit that corresponds to a "1" is part of the network/ subnet number; each bit that corresponds to "0" is part of the host number.
Gateway	The IP address of the router at the next hop to which matching frames are forwarded.
Interface	The local interface through which the next hop of this route is reached.
Metric	When a router receives a routing update that contains a new or changed destination network entry, the router adds 1 to the metric value indicated in the update and enters the network in the routing table.

Note: Most modern routers support RIP-2 so there is usually no need for a static route table.

Firewall

The Barricade's firewall enables access control of client PCs, blocks common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding. The firewall does not significantly affect system performance and we advise leaving it enabled to protect your network.

Note: When you check a radio button in the "Enable or disable Firewall module function" field, be sure to click the "APPLY" button.

Access Control

Access Control allows users to define the outgoing traffic permitted or

not-permitted through the WAN interface. The default is to permit all outgoing traffic. (See the following page for details.)

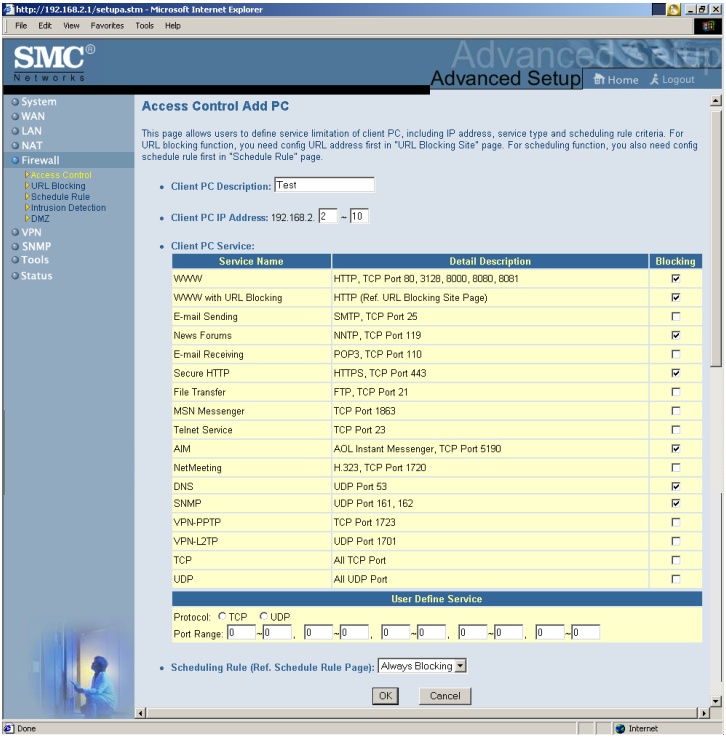
The Barricade can also limit the access of hosts within the local area network (LAN.) The MAC Filtering Table allows the Barricade to enter up to 32 MAC addresses that are not allowed access to the WAN port.

The following items are on the "Access Control" screen:

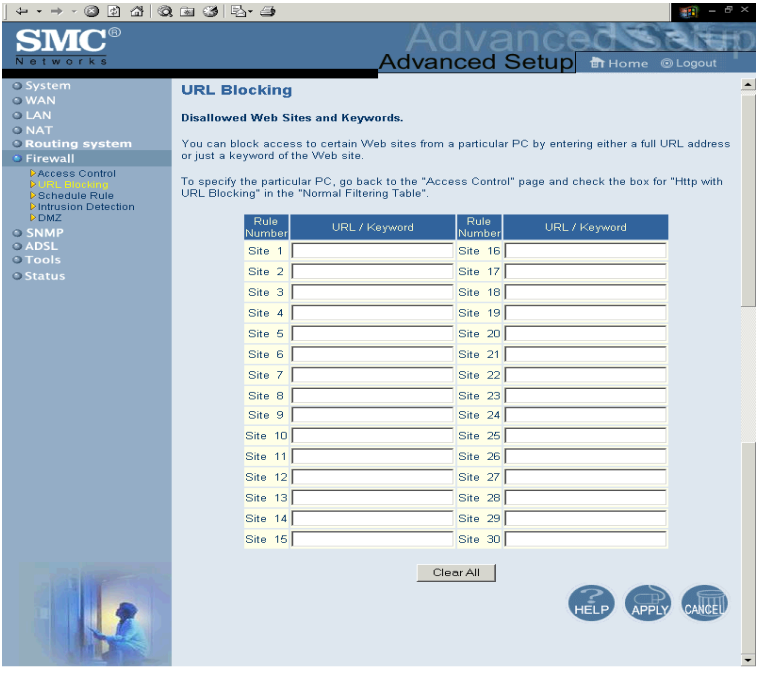
Parameter	Description
Normal Filtering Table	Displays the IP address (or an IP address range) filtering table.
MAC Filtering Table	Displays the MAC (Media Access Control) address filtering table.

Note: Click "Add PC" and define the appropriate settings for client PC services. (As shown on the following screen.)

Access Control: Add PC

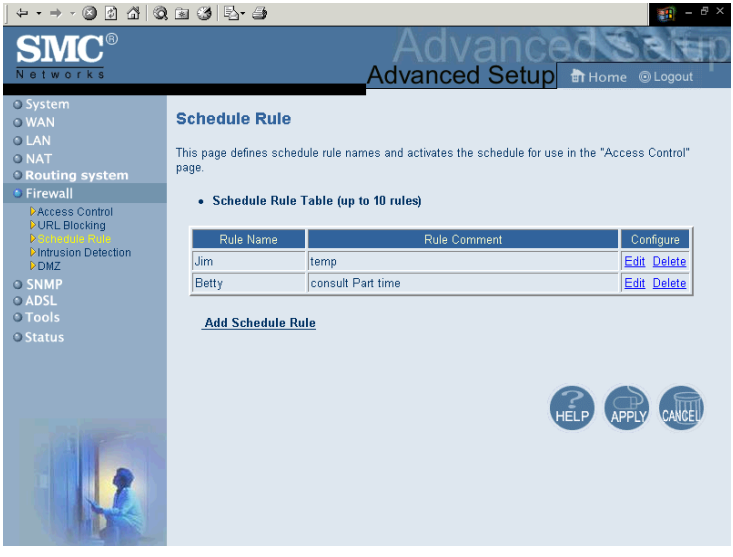

http://192.168.2.1/setupa.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
SMC Networks
Advanced Setup
Home Logout
System
WAN
LAN
NAT
Firewall
Access Control
URL Blocking
Schedule Rule
Intrusion Detection
DMZ
VPN
SNMP
Tools
Status
Access Control Add PC
This page allows users to define service limitation of client PC, including IP address, service type and scheduling rule criteria. For URL blocking function, you need config URL address first in "URL Blocking Site" page. For scheduling function, you also need config schedule rule first in "Schedule Rule" page.
Client PC Description: Test
Client PC IP Address: 192.168.2. 2 ~ 10
Client PC Service:
Service Name | Detail Description | Blocking
WWW | HTTP, TCP Port 80, 3128, 8000, 8080, 8081 | ☑
WWW with URL Blocking | HTTP (Ref. URL Blocking Site Page) | ☑
E-mail Sending | SMTP, TCP Port 25 | ☐
News Forums | NNTP, TCP Port 119 | ☑
E-mail Receiving | POP3, TCP Port 110 | ☐
Secure HTTP | HTTPS, TCP Port 443 | ☑
File Transfer | FTP, TCP Port 21 | ☐
MSN Messenger | TCP Port 1863 | ☐
Telnet Service | TCP Port 23 | ☐
AIM | AOL Instant Messenger, TCP Port 5190 | ☑
NetMeeting | H.323, TCP Port 1720 | ☐
DNS | UDP Port 53 | ☑
SNMP | UDP Port 161, 162 | ☑
VPN-PPTP | TCP Port 1723 | ☐
VPN-L2TP | UDP Port 1701 | ☐
TCP | All TCP Port | ☐
UDP | All UDP Port | ☐
User Define Service
Protocol: TCP UDP
Port Range: 0 ~ 0 , 0 ~ 0 , 0 ~ 0 , 0 ~ 0 , 0 ~ 0 , 0 ~ 0 , 0 ~ 0
Scheduling Rule (Ref. Schedule Rule Page): Always Blocking
OK
Cancel
Done
Internet

URL Blocking



The Barricade allows the user to block access to Web sites from a particular PC by entering either a full URL address or just a keyword. This feature can be used to protect children from accessing violent or pornographic web sites.

Schedule Rule



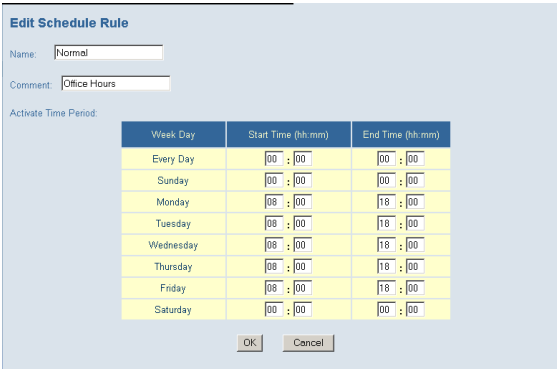
You may filter Internet access for local clients based on rules.

Each access control rule may be activated at a scheduled time. Define the schedule on the "Schedule Rule" page, and apply the rule on the "Access Control" page.

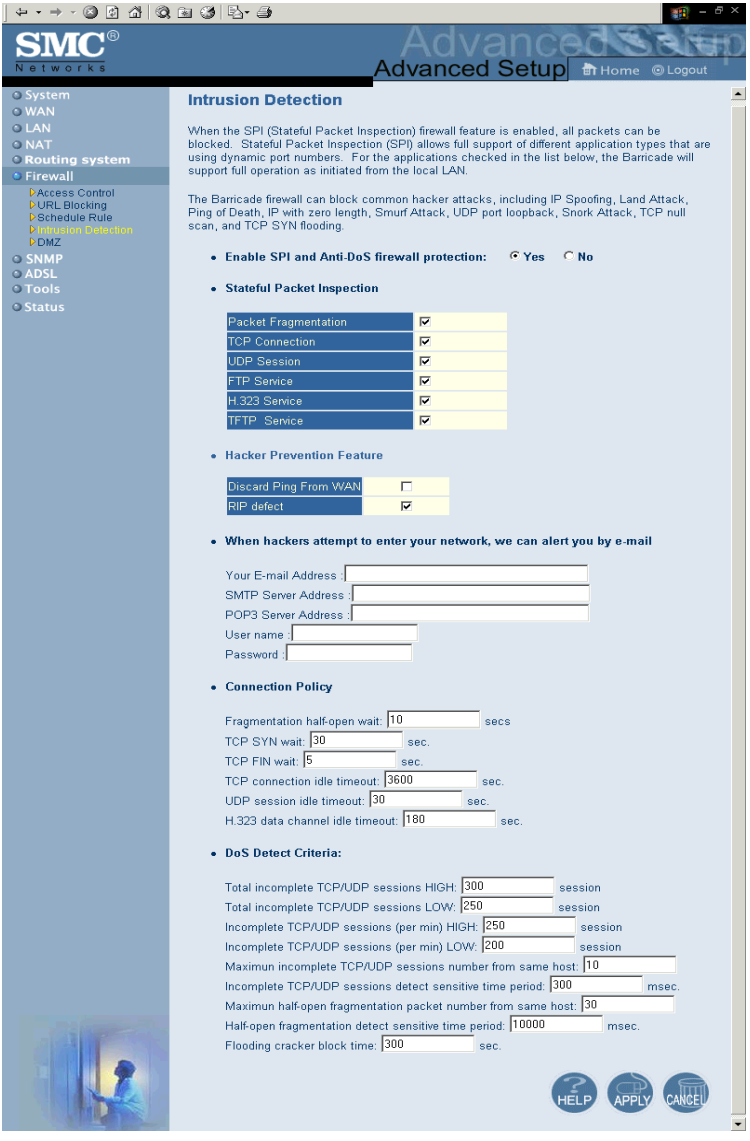
1. Click "Add Schedule Rule."

2. Define the appropriate settings for a schedule rule. (As shown on the following screen.)

3. Click “OK” and then click “APPLY” to save your settings.)


Edit Schedule Rule
Name: Normal
Comment: Office Hours
Activate Time Period:
Week Day
Start Time (hh:mm)
End Time (hh:mm)
Every Day 00 : 00 00 : 00
Sunday 00 : 00 00 : 00
Monday 08 : 00 18 : 00
Tuesday 08 : 00 18 : 00
Wednesday 08 : 00 18 : 00
Thursday 08 : 00 18 : 00
Friday 08 : 00 18 : 00
Saturday 00 : 00 00 : 00
OK
Cancel

Intrusion Detection


SMC Networks
Advanced Setup
Home
Logout
System
WAN
LAN
NAT
Routing system
Firewall
Access Control
URL Blocking
Schedule Rule
Intrusion Detection
DMZ
SNMP
ADSL
Tools
Status
Intrusion Detection
When the SPI (Stateful Packet Inspection) firewall feature is enabled, all packets can be blocked. Stateful Packet Inspection (SPI) allows full support of different application types that are using dynamic port numbers. For the applications checked in the list below, the Barricade will support full operation as initiated from the local LAN.
The Barricade firewall can block common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding.
Enable SPI and Anti-DoS firewall protection: Yes No
Stateful Packet Inspection
Packet Fragmentation
TCP Connection
UDP Session
FTP Service
H.323 Service
TFTP Service
Hacker Prevention Feature
Discard Ping From WAN
RIP defect
When hackers attempt to enter your network, we can alert you by e-mail
Your E-mail Address :
SMTP Server Address :
POP3 Server Address :
User name :
Password :
Connection Policy
Fragmentation half-open wait: 10 secs
TCP SYN wait: 30 sec.
TCP FIN wait: 5 sec.
TCP connection idle timeout: 3600 sec.
UDP session idle timeout: 30 sec.
H.323 data channel idle timeout: 180 sec.
DoS Detect Criteria:
Total incomplete TCP/UDP sessions HIGH: 300 session
Total incomplete TCP/UDP sessions LOW: 250 session
Incomplete TCP/UDP sessions (per min) HIGH: 250 session
Incomplete TCP/UDP sessions (per min) LOW: 200 session
Maximun incomplete TCP/UDP sessions number from same host: 10
Incomplete TCP/UDP sessions detect sensitive time period: 300 msec.
Maximun half-open fragmentation packet number from same host: 30
Half-open fragmentation detect sensitive time period: 10000 msec.
Flooding cracker block time: 300 sec.
HELP
APPLY
CANCEL

The Barricade's firewall inspects packets at the application layer, maintains TCP and UDP session information including timeouts and number of active sessions, and provides the ability to detect and prevent certain types of network attacks such as DoS attacks.

Network attacks that deny access to a network device are called Denial-of-Service (DoS) attacks. Denial of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources.

The Barricade protects against the following DoS attacks: Ping of Death (Ping flood) attack, SYN flood attack, IP fragment attack (Teardrop Attack), Brute-force attack, Land Attack, IP Spoofing attack, IP with zero length, TCP null scan (Port Scan Attack), UDP port loopback, Snork Attack etc.

Note: The firewall does not significantly affect system performance, so we advise enabling the prevention features to protect your network.

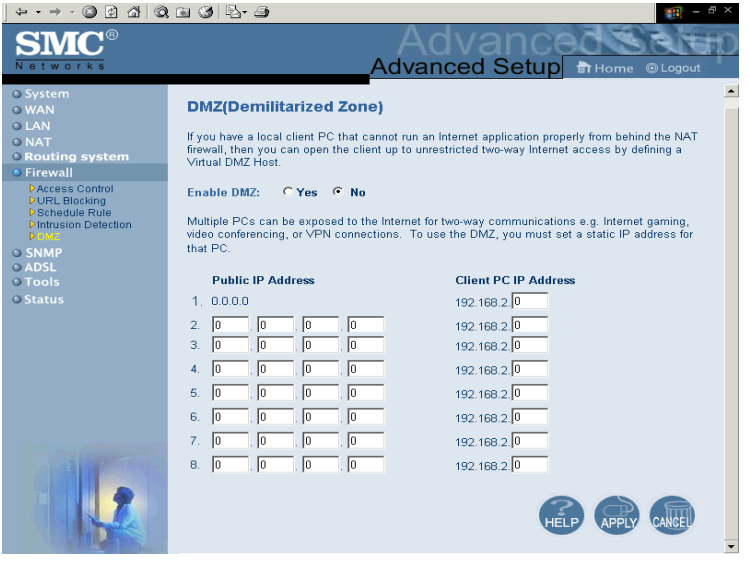
Parameter	Defaults	Description
Enable SPI and Anti-DoS firewall protection	Yes	The Intrusion Detection feature of the Barricade limits the access of the incoming traffic at the WAN port. When the SPI feature is turned on, all incoming packets are blocked except those types marked with a check in the Stateful Packet Inspection section at the top of the screen.

Parameter	Defaults	Description
Stateful Packet Inspection		This option allows you to select different application types that are using dynamic port numbers. If you wish to use Stateful Packet Inspection (SPI) for blocking packets, click on the "Yes" radio button in the "Enable SPI and Anti-DoS firewall protection" field and then check the inspection type that you need, such as Packet Fragmentation, TCP Connection, UDP Session, FTP Service, H.323 Service, and TFTP Service. It is called a "stateful" packet inspection because it examines the contents of the packet to determine what the state of the communication is, i.e. it ensures that the stated destination computer has previously requested the current communication. This is a way of ensuring that all communications are initiated by the recipient computer and are taking place only with sources that are known and trusted from previous interactions. In addition to being more rigorous in their inspection of packets, stateful inspection firewalls also close off ports until connection to the specific port is requested. When particular types of traffic are checked, only the particular type of traffic initiated from the Internal LAN will be allowed. For example, if the user only checks "FTP Service" in the Stateful Packet Inspection section, all incoming traffic will be blocked except FTP connections initiated from the local LAN.
Hacker Prevention Feature		
Discard Ping from WAN	Discard	Prevents a PING on the Gateway's WAN port from being routed to the network.

Parameter	Defaults	Description
RIP Defect	Enabled	If an IPX RIP request packet is not replied to by the router, it will stay in the input queue and not be released. Accumulated packets could cause the input queue to fill, causing severe problems for all protocols. Enabling this feature prevents the packets accumulating.
When hackers attempt to enter your network, we can alert you by e-mail		
Your E-Mail Address		Enter your e-mail address.
SMTP Server Address		Enter your SMTP server address (usually the part of the e-mail address following the "@" sign.)
POP3 Server Address		Enter your POP3 server address (usually the part of the e-mail address following the "@" sign.)
User Name		Enter your email account user name.
Password		Enter your email account password.
Connection Policy		
Fragmentation half-open wait	10 sec	Configures the number of seconds that a packet state structure remains active. When the timeout value expires, the router drops the unassembled packet, freeing that structure for use by another packet.
TCP SYN wait	30 sec	Defines how long the software will wait for a TCP session to reach an established state before dropping the session.
TCP FIN wait	5 sec	Specifies how long a TCP session will be managed after the firewall detects a FIN-exchange.
TCP connection idle timeout	3600 seconds (1 hour)	The length of time for which a TCP session will be managed if there is no activity.
UDP session idle timeout	30 sec	The length of time for which a UDP session will be managed if there is no activity.

Parameter	Defaults	Description
H.323 data channel idle timeout	180 sec	The length of time for which an H.323 session will be managed if there is no activity.
DoS Detect Criteria		
Total incomplete TCP/UDP sessions HIGH	300 sessions	Defines the rate of new unestablished sessions that will cause the software to *start* deleting half-open sessions.
Total incomplete TCP/UDP sessions LOW	250 sessions	Defines the rate of new unestablished sessions that will cause the software to *stop* deleting half-open sessions.
Incomplete TCP/UDP sessions (per min) HIGH	250 sessions	Maximum number of allowed incomplete TCP/UDP sessions per min.
Incomplete TCP/UDP sessions (per min) LOW	200 sessions	Set this to 0 as no minimum setting is required and setting it to anything higher will adversly affect performance.
Maximum incomplete TCP/UDP sessions number from same host	10	Maximum number of incomplete TCP/UDP sessions from the same host.
Incomplete TCP/UDP sessions detect sensitive time period	300 msec	Length of time before an incomplete TCP/UDP session is detected as incomplete.
Maximum half-open fragmentation packet number from same host	30	Maximum number of half-open fragmentation packets from the same host.
Half-open fragmentation detect sensitive time period	10000 msec	Length of time before a half-open fragmentation session is detected as half-open.
Flooding cracker block time	300 sec	Length of time from detecting a flood attack to blocking of the attack.

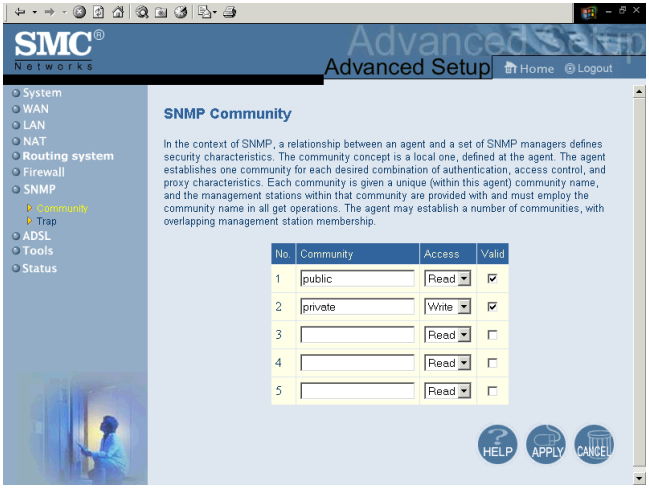
DMZ



If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. Enter the IP address of a DMZ (Demilitarized Zone) host on this screen. Adding a client to the DMZ may expose your local network to a variety of security risks, so only use this option as a last resort.

SNMP

Community

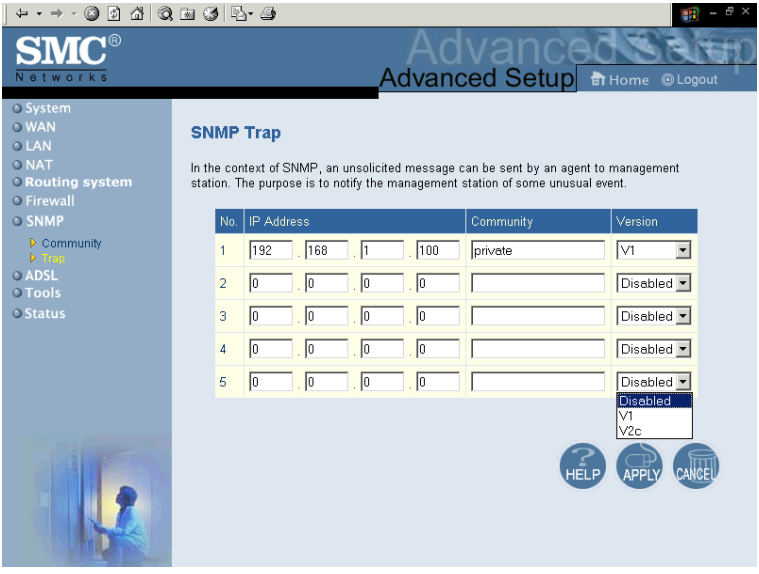


Use the SNMP configuration screen to display and modify parameters for the Simple Network Management Protocol (SNMP.) A computer attached to the network, called a Network Management Station (NMS), can be used to access this information. Access rights to the agent are controlled by community strings. To communicate with the Barricade, the NMS must first submit a valid community string for authentication.

Parameter	Description
Community	A community name authorized for management access.
Access	Management access is restricted to Read only (Read) or Read/Write (Write.)
Valid	Enables/disables the entry.

Note: Up to 5 community names may be entered.

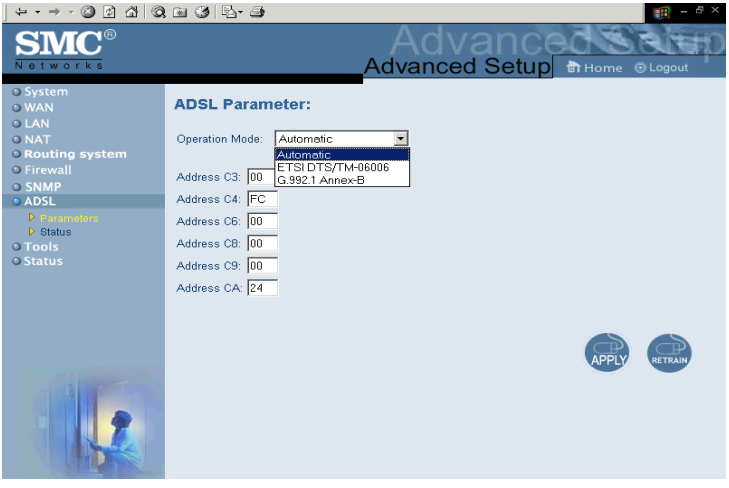
Trap



Parameter	Description
IP Address	Traps are sent to this address when errors or specific events occur on the network.
Community	A community string (password) specified for trap management. Enter a word, something other than public or private, to prevent unauthorized individuals from reading information on your system.
Version	Sets the trap status to disabled, or enabled with V1 or V2c. The v2c protocol was proposed in late 1995 and includes enhancements to v1 that are universally accepted. These include a get-bulk command to reduce network management traffic when retrieving a sequence of MIB variables, and a more elaborate set of error codes for improved reporting to a Network Management Station.

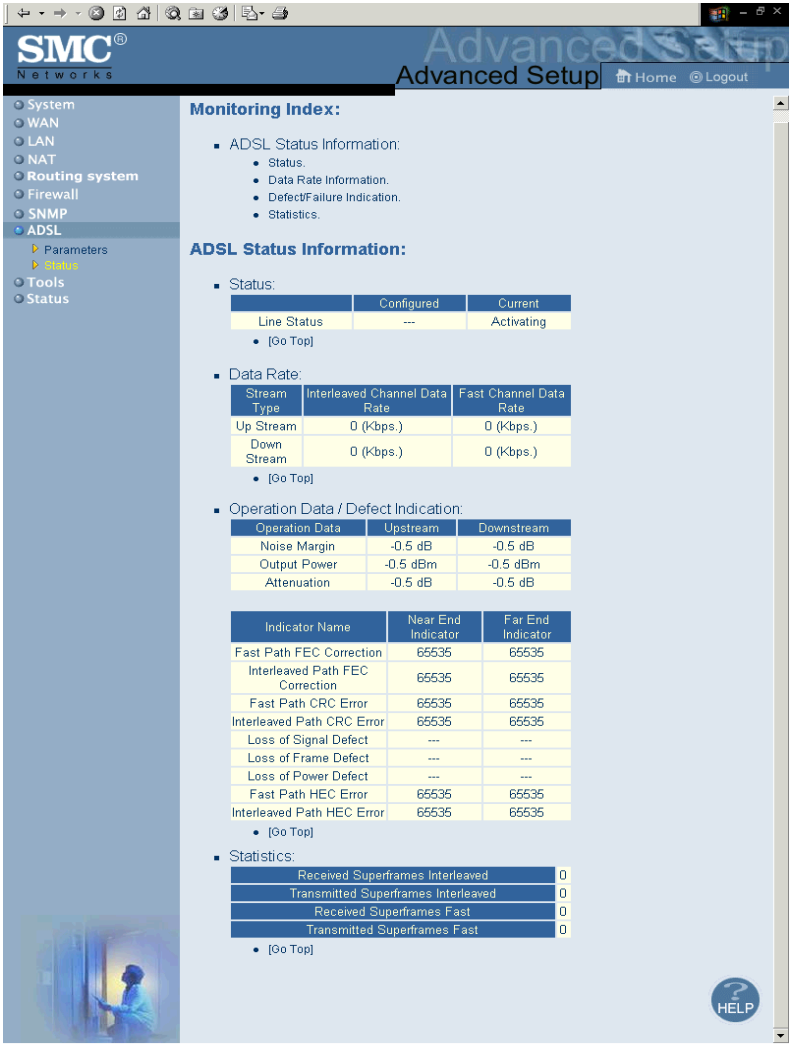
ADSL

Parameters



Parameter	Description
Operation Mode	• Automatic • ETSI DTS/TM-06006 standard. • G.992.1 standard
Address 3C etc.	Reserved.

Status


SMC Networks
Advanced Setup
Home
Logout
System
WAN
LAN
NAT
Routing system
Firewall
SNMP
ADSL
Parameters
Status
Tools
Status
Monitoring Index:
ADSL Status Information:
Status.
Data Rate Information.
Defect/Failure Indication.
Statistics.
ADSL Status Information:
Status:
Configured
Current
Line Status

Activating
[Go Top]
Data Rate:
Stream Type
Interleaved Channel Data Rate
Fast Channel Data Rate
Up Stream
0 (Kbps.)
0 (Kbps.)
Down Stream
0 (Kbps.)
0 (Kbps.)
[Go Top]
Operation Data / Defect Indication:
Operation Data
Upstream
Downstream
Noise Margin
-0.5 dB
-0.5 dB
Output Power
-0.5 dBm
-0.5 dBm
Attenuation
-0.5 dB
-0.5 dB
Indicator Name
Near End Indicator
Far End Indicator
Fast Path FEC Correction
65535
65535
Interleaved Path FEC Correction
65535
65535
Fast Path CRC Error
65535
65535
Interleaved Path CRC Error
65535
65535
Loss of Signal Defect

Loss of Frame Defect

Loss of Power Defect

Fast Path HEC Error
65535
65535
Interleaved Path HEC Error
65535
65535
[Go Top]
Statistics:
Received Superframes Interleaved
0
Transmitted Superframes Interleaved
0
Received Superframes Fast
0
Transmitted Superframes Fast
0
[Go Top]
HELP

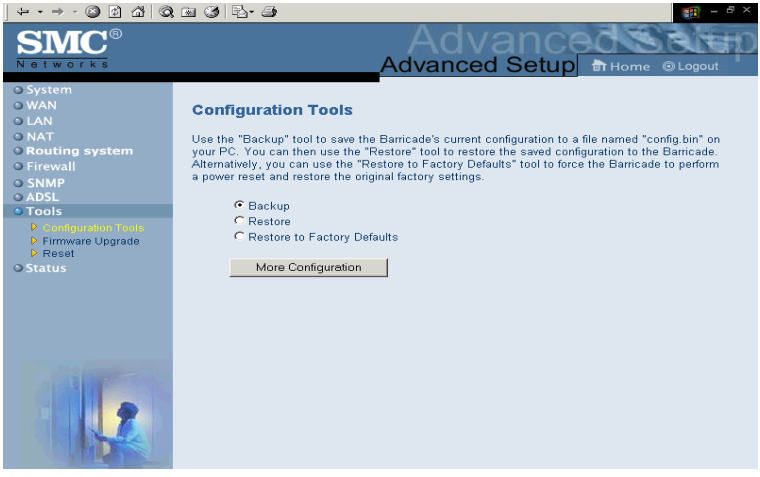
Parameter	Description
Status	
Line Status	Shows the current status of the ADSL line.
Data Rate	
Upstream	Actual and maximum upstream data rate.
Downstream	Actual and maximum downstream data rate.
Operation Data/ Defect Indication	
Noise Margin	
Upstream:	Minimum noise margin upstream.
Downstream:	Minimum noise margin downstream.
Output Power	Maximum fluctuation in the output power.
Attenuation	
Upstream:	Maximum reduction in the strength of the upstream signal.
Downstream:	Maximum reduction in the strength of the downstream signal.
Fast Path FEC Correction	There are two latency paths that may be used: fast and interleaved. For either path a forward error correction (FEC) scheme is employed to ensure higher data integrity. For maximum noise immunity, an interleaver may be used to supplement FEC.
Interleaved Path FEC Correction	An interleaver is basically a buffer used to introduce a delay, allowing for additional error correction techniques to handle noise. Interleaving slows the data flow and may not be optimal for real time signals such as video transmission.
Fast Path CRC Error	Indicates the number of Fast Path Cyclic Redundancy Check errors.
Interleaved Path CRC Error	Indicates the number of Interleaved Path Cyclic Redundancy Check errors.

Parameter	Description
Loss of Signal Defect	Momentary signal discontinuities.
Loss of Frame Defect	Failures due to loss of frames.
Loss of Power Defect	Failures due to loss of power.
Fast Path HEC Error	Fast Path Header Error Concealment errors.
Interleaved Path HEC Error	Interleaved Path Header Error Concealment errors.
Statistics	Superframes represent the highest level of data presentation. Each superframe contains regular ADSL frames, one of which is used to provide superframe synchronization, identifying the start of a superframe. Some of the remaining frames are also used for special functions.
Received Superframes Interleaved	Number of interleaved Superframes received.
Transmitted Superframes Interleaved	Number of interleaved Superframes transmitted.
Received Superframes Fast	Number of fast Superframes received.
Transmitted Superframes Fast	Number of fast Superframes transmitted.

Tools

Use the "Tools" menu to backup the current settings, to restore previously saved settings, or restore the factory default settings.

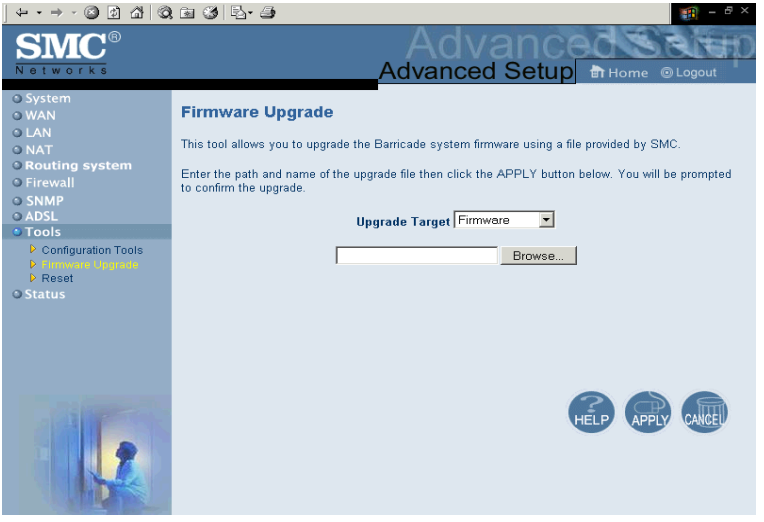
Configuration Tools



Check "Backup" and click "More Configuration" to save your Barricade's configuration to a file named config.bin on your PC. You can then check the "Restore" radio button and click "More Configuration" to restore the saved backup configuration file.

To restore the factory settings, check "Restore to Factory Defaults" and click "More Configuration." You will be asked to confirm your decision.

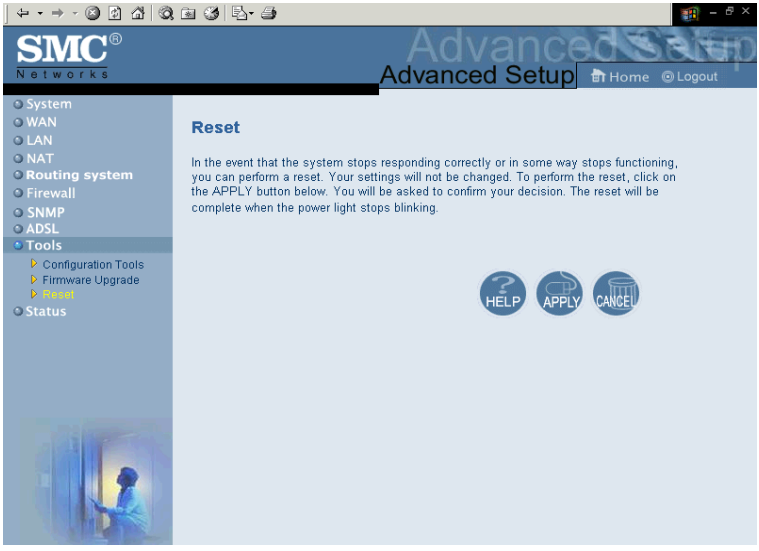
Firmware Upgrade



Use this screen to update the firmware or user interface to the latest versions. In the "Upgrade Target" field, choose "Firmware" or "User Interface" depending on which you want to update. Then click "Browse" to browse for the previously downloaded file.

Note: For latest firmware/user interface version information and download, visit SMC's Web site at www.smc-europe.com.

Reset

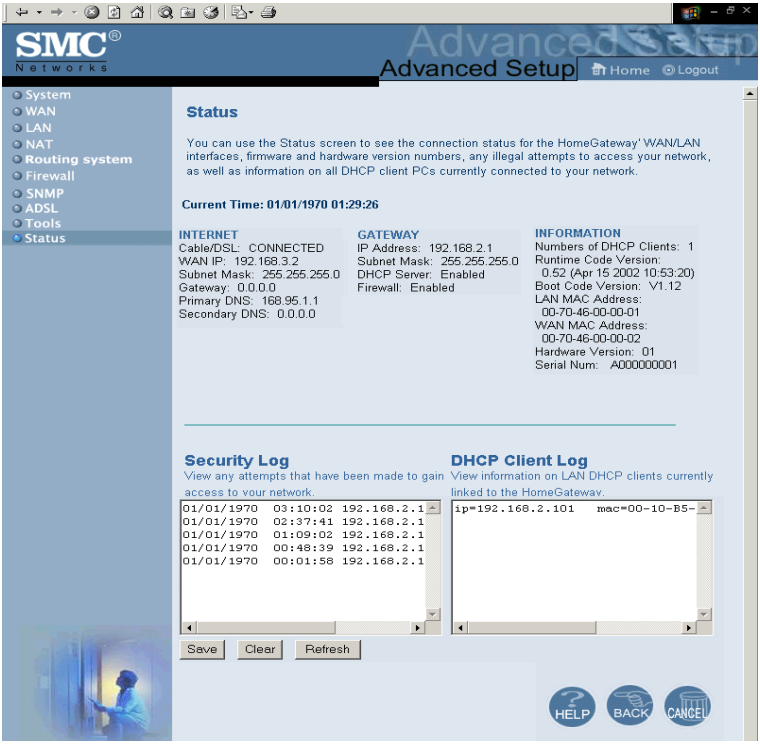


Perform a reset from this page. The configurations will not be changed back to the factory default settings.

Note: If you use the reset button on the rear panel, the Barricade performs a power reset and restores the factory settings.

Status

The Status screen displays WAN/LAN connection status, firmware and hardware version numbers, as well as information on DHCP clients connected to your network.



The security log may be saved to a file by clicking "Save" and choosing a location.

The following items are included on this screen:

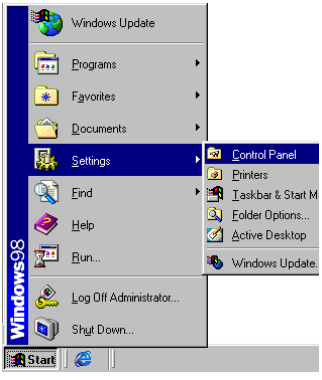
Parameter	Description
INTERNET	Displays WAN connection type and status.
GATEWAY	Displays system IP settings, as well as DHCP Server and Firewall status.
INFORMATION	Displays the number of attached clients, the firmware versions, the physical MAC address for each media interface, and for the Barricade, as well as the hardware version and serial number.
Security Log	Displays illegal attempts to access your network.
DHCP Client Log	Displays information on DHCP clients on your network.

CHAPTER 5
CONFIGURING CLIENT TCP/IP

After completing hardware setup by connecting all your network devices, you need to configure your computer to connect to the Barricade. First determine how your ISP issues your IP address. Many ISPs issue these numbers automatically using Dynamic Host Configuration Protocol (DHCP.) Other ISPs provide a static IP address and associated numbers, which you must enter manually. How your ISP assigns your IP address determines how you need to configure your computer. See this section for Windows 95/98/Me configuration. See "Windows NT 4.0" on page 5-6, "Windows 2000" on page 5-11, "Windows XP" on page 5-15, or "Configuring Your Macintosh Computer" on page 5-19 depending on your operating system.

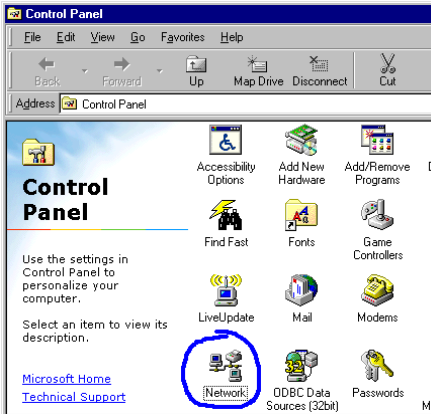
Windows 95/98/Me

You may find that the instructions in this section do not exactly match your version of Windows. This is because these steps and screenshots were created from Windows 98. Windows 95 and Windows Millennium Edition are similar, but not identical, to Windows 98.



1. From the Windows desktop, click the "Start" button. Choose "Settings," and then click "Control Panel."

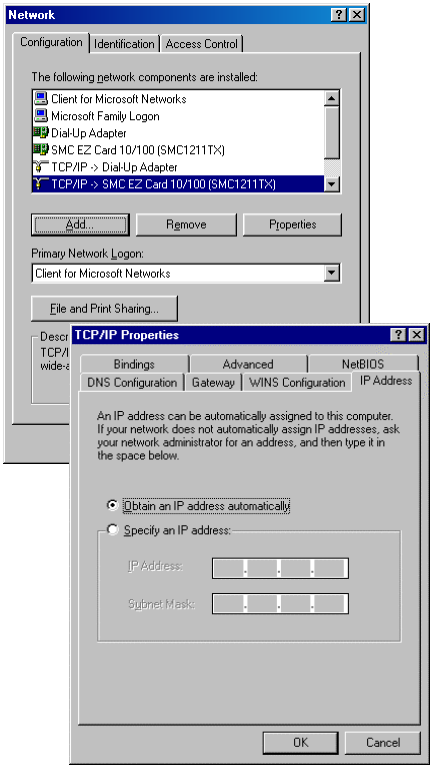
2. In “Control Panel” double-click the “Network” icon.



3. In the “Network” window, under the “Configuration” tab, double-click the “TCP/IP” item listed for your network card.

4. Select the “IP Address” tab.

5. If “Obtain an IP address automatically” is already selected, your computer is already configured for DHCP. Click “Cancel” to close each window, and skip to “Disable HTTP Proxy” on page 5-4.” If not, locate your IP address and subnet mask. Record the numbers in the space provided on the following page.

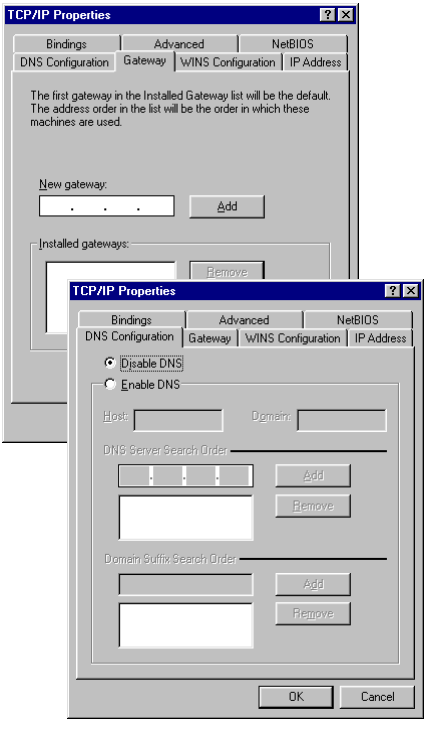

Network
Configuration Identification Access Control
The following network components are installed:
Client for Microsoft Networks
Microsoft Family Logon
Dial-Up Adapter
SMC EZ Card 10/100 (SMC1211TX)
TCP/IP -> Dial-Up Adapter
TCP/IP -> SMC EZ Card 10/100 (SMC1211TX)
Add... Remove Properties
Primary Network Logon:
Client for Microsoft Networks
File and Print Sharing...
TCP/IP Properties
Bindings Advanced NetBIOS
DNS Configuration Gateway WINS Configuration IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK Cancel

6. Click the "Gateway" tab and record the numbers listed under "Installed gateways."

7. Click the "DNS Configuration" tab. Locate the DNS servers listed under "DNS Server Search Order." Record any listed addresses.

8. After writing down your settings, check to make sure you have recorded them correctly. Click the "IP Address" tab and then click "Obtain an IP address automatically." Click "OK."

9. Windows may need your Windows 95/98/Me CD to copy some files. After it finishes copying, it will prompt you to restart your system. Click "Yes" and your computer will shut down and restart.



System Settings Change
You must restart your computer before the new settings will take effect.
Do you want to restart your computer now?
Yes
No

TCP/IP Configuration Setting

IP Address	_____._____._____._____
Subnet Mask	_____._____._____._____
Primary DNS Server	_____._____._____._____
Secondary DNS Server	_____._____._____._____
Default Gateway	_____._____._____._____
Host Name	_____._____._____._____

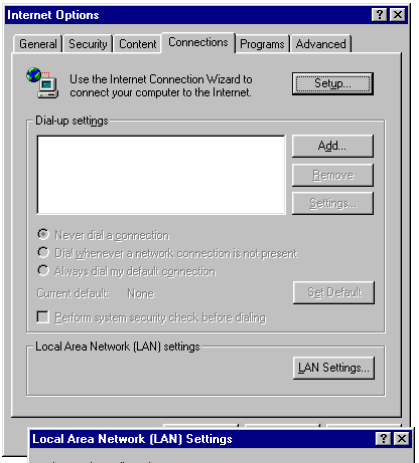
Disable HTTP Proxy

You need to verify that the "HTTP Proxy" feature of your Web browser is disabled. This is so that your browser can view the Barricade's HTML configuration pages. The following steps are for Internet Explorer and Netscape. Determine which browser you use and follow the appropriate steps.

Internet Explorer

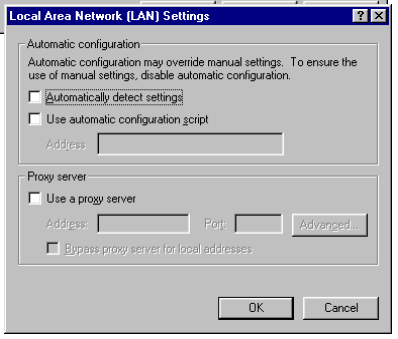
1. Open Internet Explorer and click the stop button. Click "Tools," then "Internet Options."

2. In the "Internet Options" window, click the "Connections" tab. Next, click the "LAN Settings..." button.

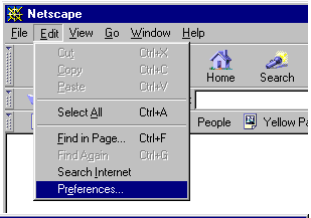


3. Clear all the checkboxes.

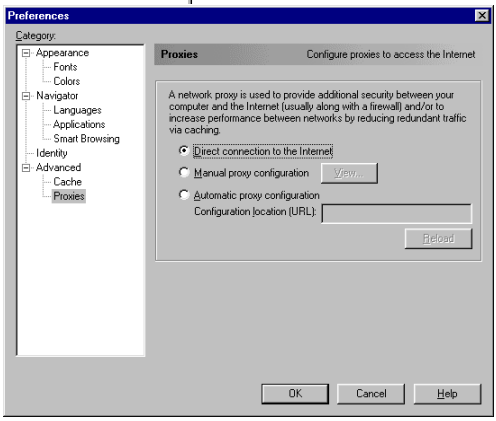
4. Click "OK," and then click "OK" again to close the "Internet Options" window.


Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
Proxy server
Use a proxy server
Address: Port: Advanced...
Bypass proxy server for local addresses
OK
Cancel

Netscape



1. Open Netscape and click the stop button. Click "Edit," then click "Preferences..."



2. In the "Preferences" window, under "Category" double-click "Advanced," then click "Proxies." Select "Direct connection to the Internet." Click "OK."

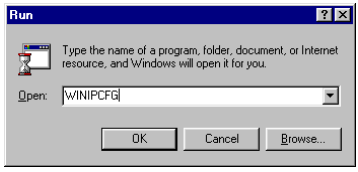
3. Repeat these steps for each Windows 95/98/Me computer connected to your Barricade.

Obtain IP Settings from Your ADSL Router

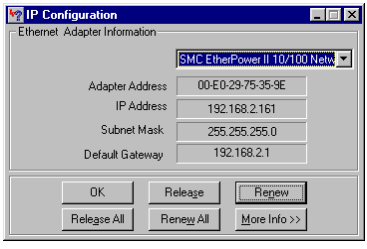
Now that you have configured your computer to connect to your Barricade, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your Barricade, you can also verify that you have configured your computer correctly.

1. Click "Start," then "Run..."

2. Type "WINIPCFG" and click "OK." It may take a second or two for the "IP Configuration" window to appear.



3. From the drop-down menu, select your network card. Click "Release" and then "Renew." Verify that your IP address is now **192.168.2.xxx**, your Subnet Mask is **255.255.255.0** and your Default Gateway is **192.168.2.1**. These values confirm that your Barricade is functioning. Click "OK" to close the "IP Configuration" window.



Windows NT 4.0

After completing hardware setup by connecting your network devices, you need to configure your computer to connect to the Barricade. First determine how your ISP issues your IP address. Many ISPs issue these numbers automatically using Dynamic Host Configuration Protocol (DHCP.) Other ISPs provide a static IP address and associated numbers, which you must enter manually. How your ISP assigns your IP address determines how you need to configure your computer.

Follow these instructions:

1. From the Windows desktop click "Start/ Settings/Control Panel."

2. Double-click the "Network" icon.

3. Select the "Protocols" tab.

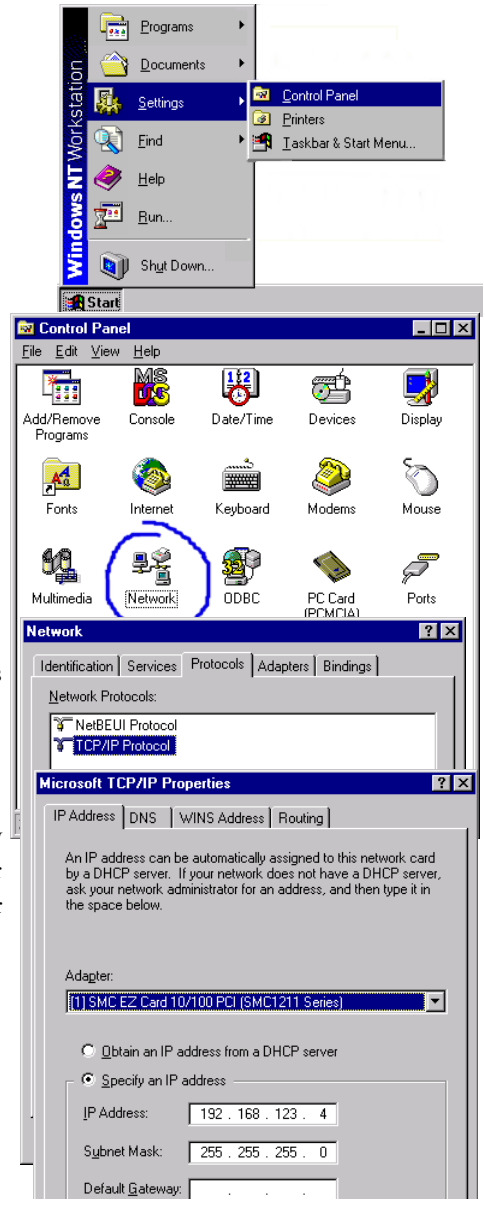
4. Double-click "TCP/IP Protocol."

5. Select the "IP Address" tab.

6. In the "Adapter" drop-down list, be sure your Ethernet adapter is selected.

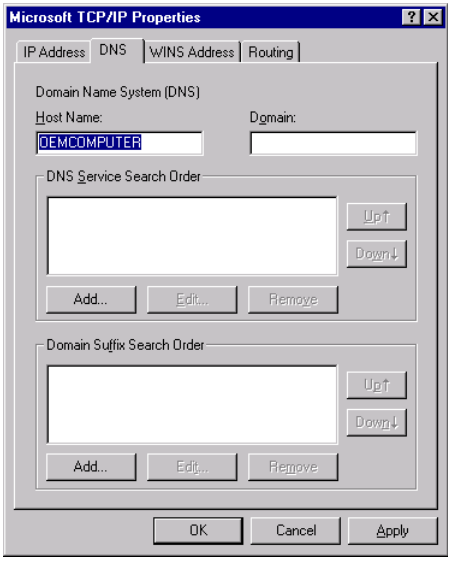
7. If "Obtain an IP address automatically" is already selected, your computer is already configured for DHCP. Click "Cancel" to close each window, and skip to "Disable HTTP Proxy" on page 5-9.

8. In the "TCP/IP Properties" dialog box,



under the IP address tab, locate your IP address, subnet mask, and default gateway. Record these values in the spaces provided below.

9. Click the "DNS" tab to see the primary and secondary DNS servers. Record these values in the spaces provided below.



10. After writing down your IP settings, click the IP address tab. Select "Obtain IP address automatically" and click "OK." Click "OK" again to close the "Network" window.

11. Windows may copy some files, and will then prompt you to restart your system. Click "Yes" and your computer will shut down and restart.

TCP/IP Configuration Setting

IP Address	____.____.____.____
Subnet Mask	____.____.____.____
Default Gateway	____.____.____.____
Primary DNS Server	____.____.____.____
Secondary DNS Server	____.____.____.____
Host Name	____.____.____.____

Disable HTTP Proxy

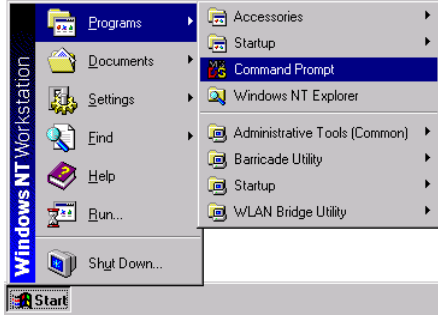
You need to verify that the "HTTP Proxy" feature of your Web browser is disabled. This is so that your browser can view the Barricade's HTML configuration pages. Determine which browser you use and refer to "Internet Explorer" on page 5-4 or "Netscape" on page 5-5.

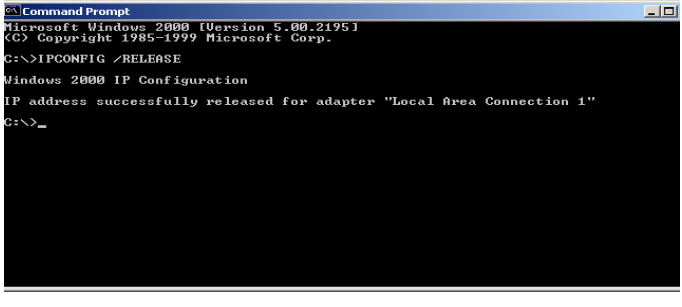
Obtain IP Settings from Your Barricade

Now that you have configured your computer to connect to your Barricade, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your Barricade, you will verify that you have configured your computer correctly.

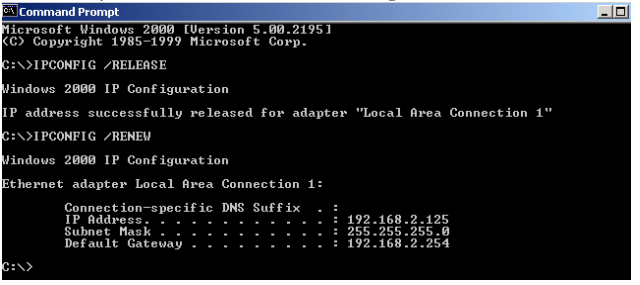
1. From the Windows desktop, click "Start/Programs/ and then click "Command Prompt."

2. In the "Command Prompt" window, type "IPCONFIG /RELEASE" and press the <ENTER> key.




Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
C:\>IPCONFIG /RELEASE
Windows 2000 IP Configuration
IP address successfully released for adapter "Local Area Connection 1"
C:\>

3. Type "IPCONFIG /RENEW" and press the <ENTER> key. Verify that your IP Address is now **192.168.2.xxx**, your Subnet Mask is **255.255.255.0** and your Default Gateway is **192.168.2.1**. These values confirm that your Barricade is functioning.

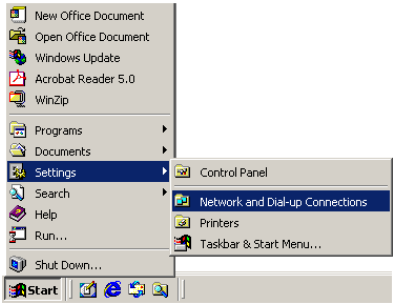

Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
C:\>IPCONFIG /RELEASE
Windows 2000 IP Configuration
IP address successfully released for adapter "Local Area Connection 1"
C:\>IPCONFIG /RENEW
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection 1:
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.2.125
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.2.254
C:\>

4. Type "EXIT" and press <ENTER> to close the "Command Prompt" window.

Your computer is now configured to connect to the Barricade.

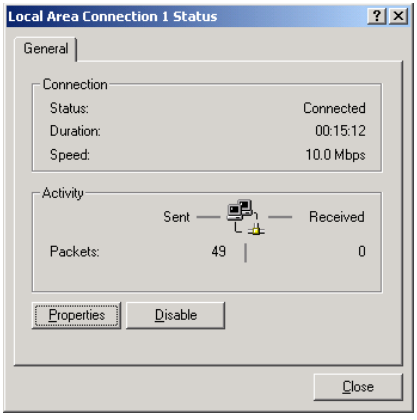
Windows 2000

1. On the Windows desktop, click "Start/Settings/ Network and Dial-Up Connections."



2. Click the icon that corresponds to the connection to your Barricade.

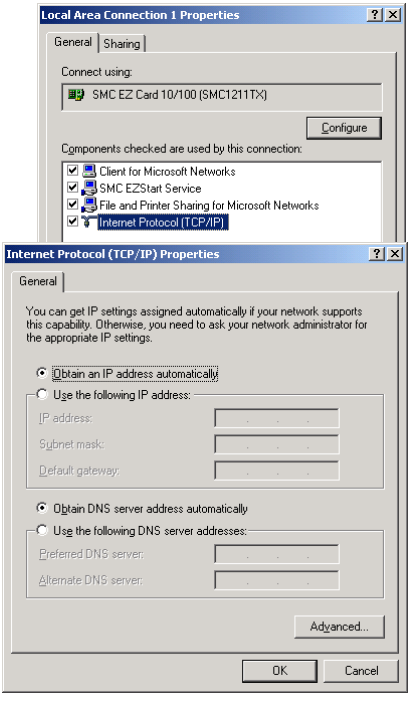
3. The connection status screen will open. Click "Properties."



4. Double-click "Internet Protocol (TCP/IP.)"

5. If there is IP Address information on the "Internet Protocol (TCP/IP) Properties" dialog box, it should be recorded. Use the spaces below to record the current settings.

6. If "Obtain an IP address automatically" and "Obtain DNS server address automatically" are already selected, your computer is already configured for DHCP. Click "Cancel" to close each window, and skip to "Disable HTTP Proxy" on page 5-13."


Local Area Connection 1 Properties
General
Sharing
Connect using:
SMC EZ Card 10/100 (SMC1211TX)
Configure
Components checked are used by this connection:
Client for Microsoft Networks
SMC EZStart Service
File and Printer Sharing for Microsoft Networks
Internet Protocol (TCP/IP)
Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

7. Select "Obtain an IP address automatically" and "Obtain DNS server address automatically." Click "OK" or "Close" to close each window.

TCP/IP Configuration Setting

IP Address	____.____.____.____
Subnet Mask	____.____.____.____
Default Gateway	____.____.____.____
Preferred DNS Server	____.____.____.____
Alternate DNS Server	____.____.____.____

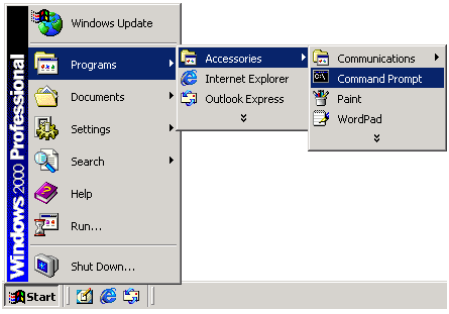
Disable HTTP Proxy

You need to verify that the "HTTP Proxy" feature of your Web browser is disabled. This is so that your browser can view the Barricade's HTML configuration pages. Determine which browser you use and refer to "Internet Explorer" on page 5-4 or "Netscape" on page 5-5.

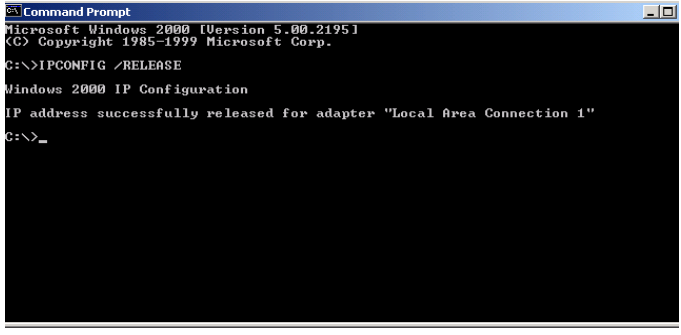
Obtain IP Settings from Your Barricade

Now that you have configured your computer to connect to your Barricade, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your Barricade, you can verify that you have configured your computer correctly.

1. From the Windows desktop, click "Start/ Programs/Accessories," and then "Command Prompt."

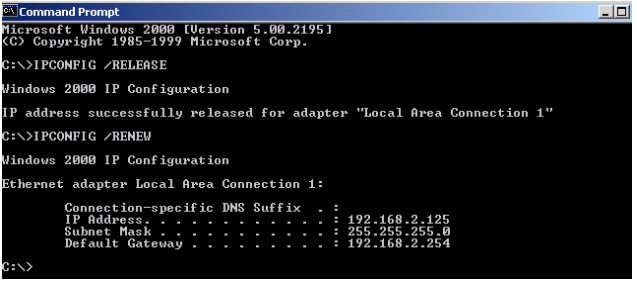


2. In the "Command Prompt" window, type "IPCONFIG/RELEASE" and press the <ENTER> key.


Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
C:\>IPCONFIG /RELEASE
Windows 2000 IP Configuration
IP address successfully released for adapter "Local Area Connection 1"
C:\>

3. Type "IPCONFIG /RENEW" and press the <ENTER> key. Verify

that your IP Address is now **192.168.2.xxx**, your Subnet Mask is **255.255.255.0** and your Default Gateway is **192.168.2.1**. These values confirm that your ADSL Router is functioning.


Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
C:\>IPCONFIG /RELEASE
Windows 2000 IP Configuration
IP address successfully released for adapter "Local Area Connection 1"
C:\>IPCONFIG /RENEW
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection 1:
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.2.125
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.2.254
C:\>

4. Type "EXIT" and press <ENTER> to close the "Command Prompt" window.

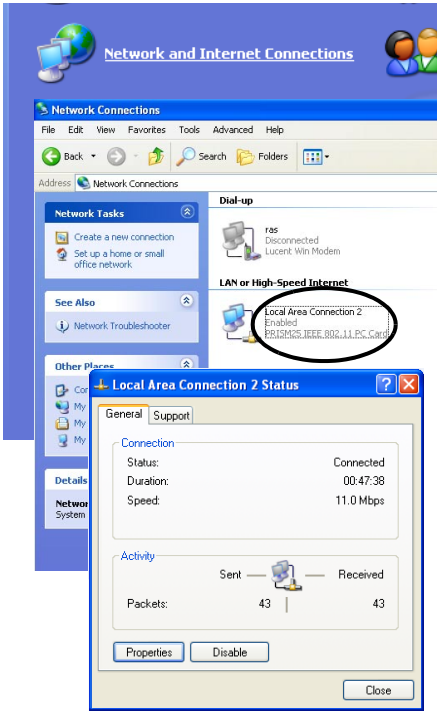
Your computer is now configured to connect to the Barricade.

Windows XP

1. Click “start/Control Panel.”

2. In “Control Panel” click “Network and Internet Connections.”

3. The “Network Connections” screen will open. Double-click the connection for this device.

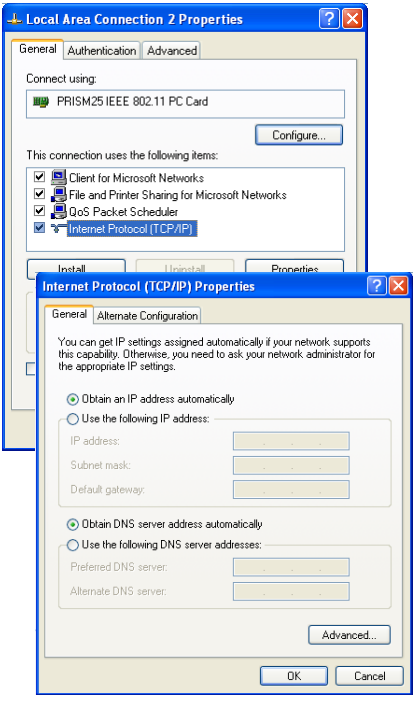


4. On the connection status screen, click “Properties.”

5. Double-click "Internet Protocol (TCP/IP.)"

6. If there is IP Address information on the "Internet Protocol (TCP/IP) Properties" dialog box, it should be recorded. Use the spaces below to record the current settings.

7. If "Obtain an IP address automatically" and "Obtain DNS server address automatically" are already selected, your computer is already configured for DHCP. Click "Cancel" to close each window, and skip to "Disable HTTP Proxy" on page 5-17."



8. Select "Obtain an IP address automatically" and "Obtain DNS server address automatically." Click "OK" or "Close" to close each window.

TCP/IP Configuration Setting

IP Address	_____._____._____._____
Subnet Mask	_____._____._____._____
Default Gateway	_____._____._____._____
Preferred DNS Server	_____._____._____._____
Alternate DNS Server	_____._____._____._____

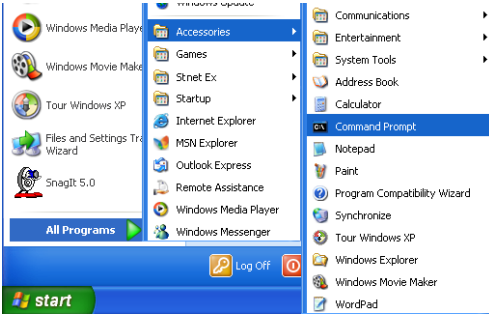
Disable HTTP Proxy

You need to verify that the "HTTP Proxy" feature of your Web browser is disabled. This is so that your browser can view the Barricade's HTML configuration pages. Determine which browser you use and refer to "Internet Explorer" on page 5-4 or "Netscape" on page 5-5.

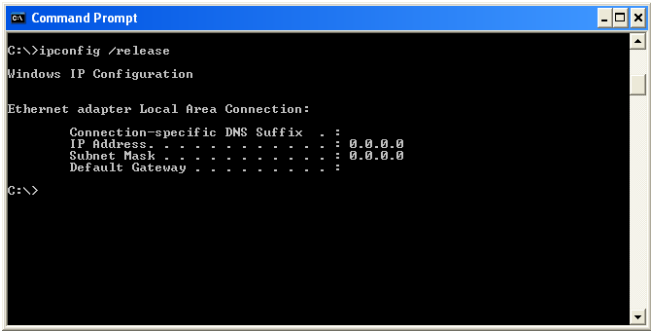
Obtain IP Settings from Your Barricade

Now that you have configured your computer to connect to your Barricade, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your Barricade, you can verify that you have configured your computer correctly.

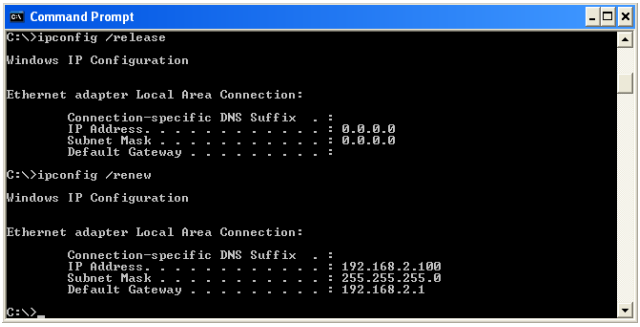
1. From the Windows desktop, click "start/ Programs/ Accessories/ Command Prompt."



2. In the "Command Prompt" window, type "IPCONFIG/RELEASE" and press the <ENTER> key.


Command Prompt
C:\>ipconfig /release
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 0.0.0.0
Subnet Mask . . . . . : 0.0.0.0
Default Gateway . . . . . :
C:\>

3. Type "IPCONFIG /RENEW" and press the <ENTER> key. Verify that your IP Address is now **192.168.2.xxx**, your Subnet Mask is **255.255.255.0** and your Default Gateway is **192.168.2.1**. These values confirm that your ADSL Router is functioning.


Command Prompt
C:\>ipconfig /release
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 0.0.0.0
Subnet Mask . . . . . : 0.0.0.0
Default Gateway . . . . . :
C:\>ipconfig /renew
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.2.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.2.1
C:\>

Type "EXIT" and press <ENTER> to close the "Command Prompt" window.

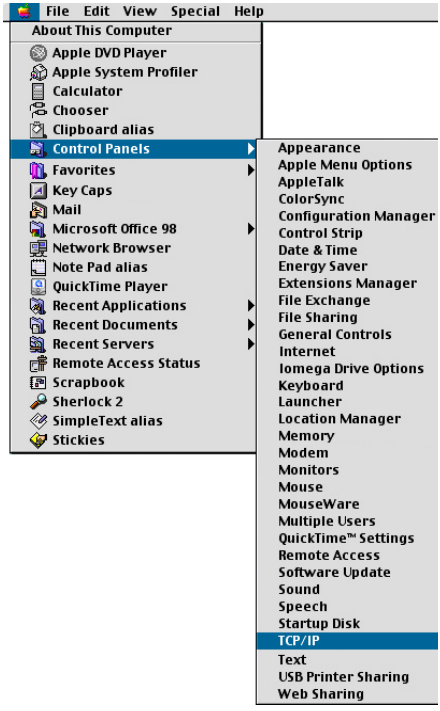
Your computer is now configured to connect to the Barricade.

Configuring Your Macintosh Computer

You may find that the instructions here do not exactly match your operating system. This is because these steps and screenshots were created using Mac OS 8.5. Mac OS 7.x and above are similar, but may not be identical to Mac OS 8.5.

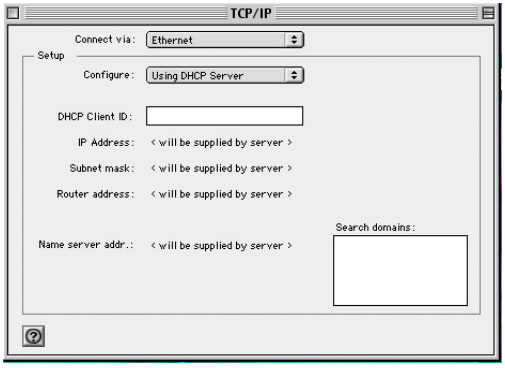
Follow these instructions:

1. Pull down the Apple Menu. Click "Control Panels" and select "TCP/IP."



2. In the TCP/IP dialog box, make sure "Ethernet" is selected in the "Connect via:" field.

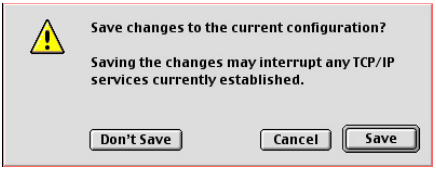
3. If "Using DHCP Server" is already selected in the "Configure" field, your computer is already configured for DHCP. Close the TCP/IP dialog box, and skip to "Disable HTTP Proxy" on page 5-21."



4. If there is IP Address information on the "TCP/IP" screen, it should be recorded. Use the spaces below to record the current settings.

5. After writing down your IP settings, select "Using DHCP Server" in the "Configure" field and close the window.

6. Another box will appear asking whether you want to save your settings. Click "Save."


Save changes to the current configuration?
Saving the changes may interrupt any TCP/IP services currently established.
Don't Save
Cancel
Save

TCP/IP Configuration Setting

IP Address _____._____._____._____

Subnet mask _____._____._____._____

Router address _____._____._____._____

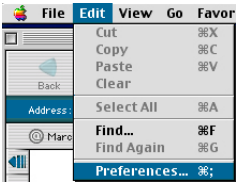
Name server addr. _____._____._____._____

Disable HTTP Proxy

You need to verify that the "HTTP Proxy" feature of your Web browser is disabled. This is so that your browser can view the Barricade's HTML configuration pages. The following steps are for Internet Explorer and Netscape. Determine which browser you use and follow the appropriate steps.

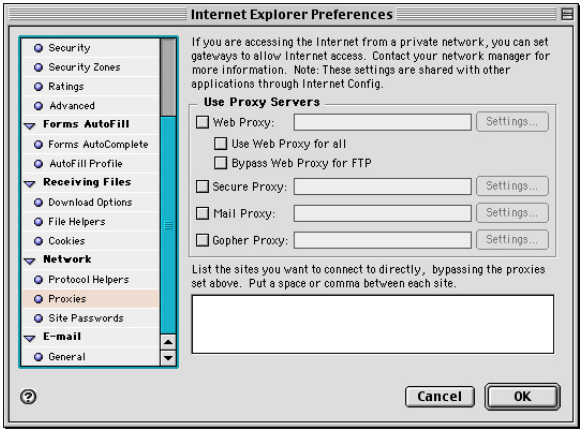
Internet Explorer

1. Open Internet Explorer and click the stop button. Click "Edit" and select "Preferences."



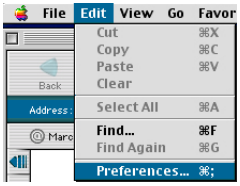
2. In the Internet Explorer Preferences window, under Network, select "Proxies."

3. Uncheck all checkboxes and click "OK."



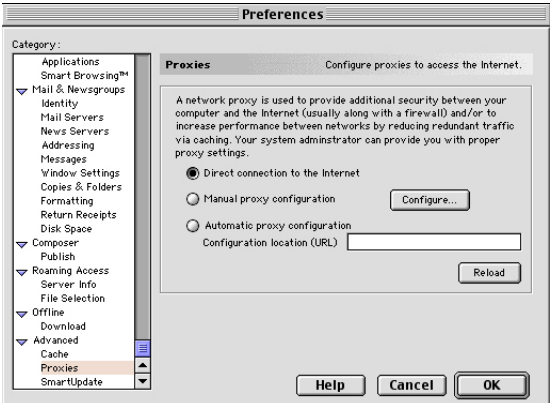
Netscape

1. Open Netscape and click the stop button. Click "Edit" and select "Preferences."



2. In the "Preferences" dialog box, in the left-hand column labeled Category," select "Advanced." Under the "Advanced" category, select "Proxies."

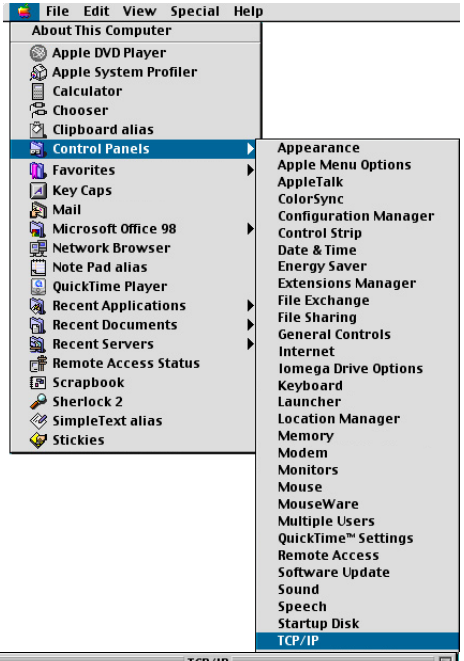
3. Select "Direct Connection to the Internet" and click "OK."



Obtain IP Settings from Your Barricade

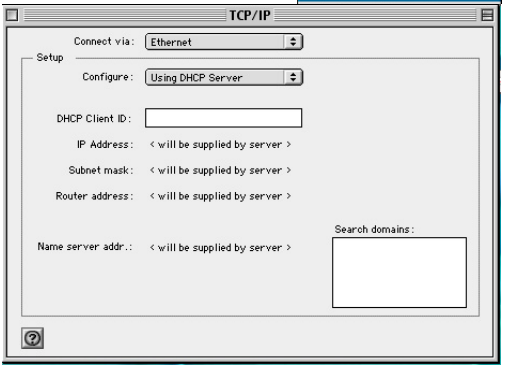
Now that you have configured your computer to connect to your Barricade, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your Barricade, you can verify that you have configured your computer correctly.

1. Pull down the Apple Menu. Click "Control Panels" and select TCP/IP.



2. Your new settings are shown in the TCP/IP window. Verify that your IP Address is now **192.168.2.xxx**, your Subnet Mask is **255.255.255.0** and your Default Gateway is **192.168.2.1**. These values confirm that your Barricade is functioning.

3. Close the TCP/IP window.



Now your computer is configured to connect to the Barricade.

CHAPTER 6
CONFIGURING PRINTER SERVICES

To use the print server built into the Barricade, you must first install the Port Monitor program as described in the following section for Windows 95/98/Me/NT/2000/XP.

To configure the Barricade Print Server for Windows 95/98/Me/NT/2000/XP or Unix, see "Configure the Print Server" on page 6-4.

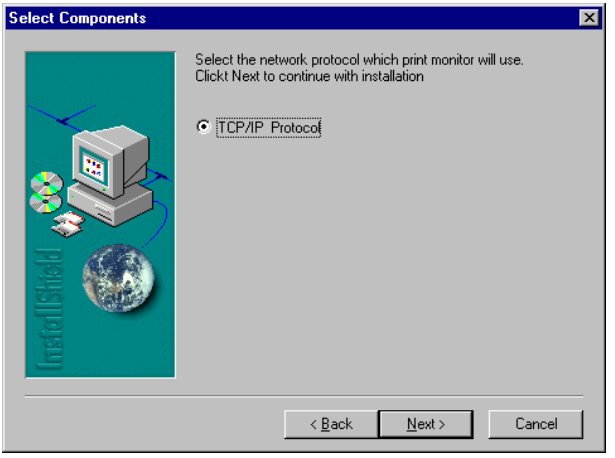
Install the Printer Port Monitor

Skip this section if you are using Unix.

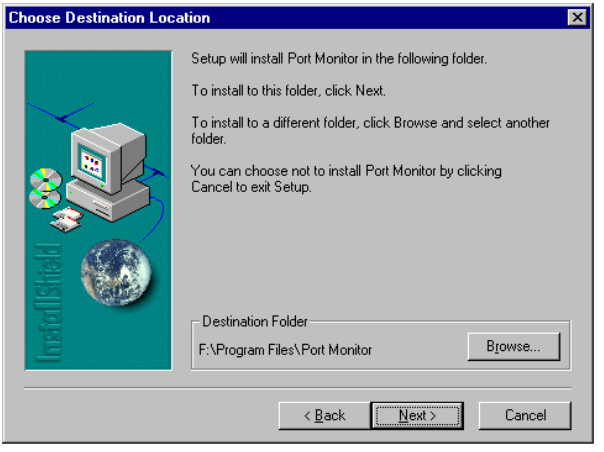
For Windows 95/98/Me/NT/2000/XP clients, you need to install the port monitor program as described in this section.

1. Insert the installation CD-ROM into your CD-ROM drive. Under the PrintSvr directory, run the "setup.exe" program. The Port Monitor installation program advises you to close all other Windows programs currently running on your computer. Click "Next" to continue.

2. The next screen indicates that the print client uses the TCP/IP network protocol to monitor print requests. Click "Next."

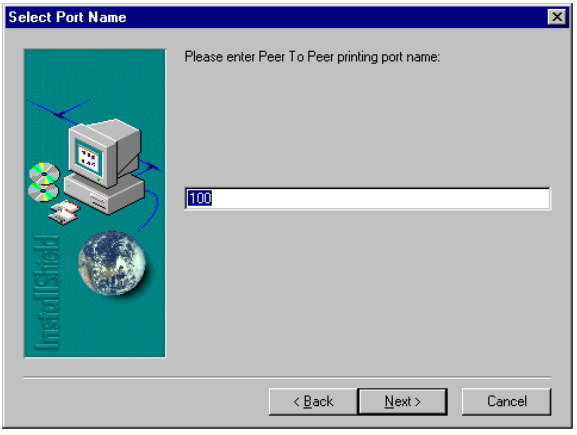


3. Select the destination folder and click on the "Next" button. The setup program will then begin to install the programs into the destination folder.

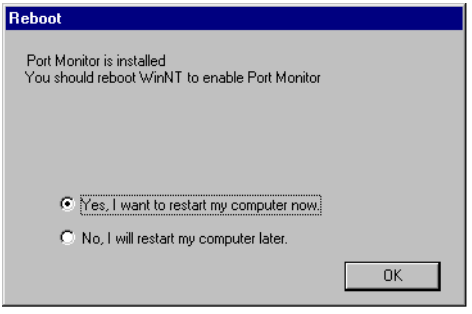

Choose Destination Location
Setup will install Port Monitor in the following folder.
To install to this folder, click Next.
To install to a different folder, click Browse and select another folder.
You can choose not to install Port Monitor by clicking Cancel to exit Setup.
InstallShield
Destination Folder
F:\Program Files\Port Monitor
Browse...
< Back
Next >
Cancel

4. Select the Program Folder that will contain the program icon for uninstalling the port monitor, and then click "Next."

5. Enter the printer port name that will be used to identify the port monitor in your system, and click "Next."



6. When the setup program finishes installing the port monitor, check "Yes, I want to restart my computer now" and then click "OK."


Reboot
Port Monitor is installed
You should reboot WinNT to enable Port Monitor
Yes, I want to restart my computer now.
No, I will restart my computer later.
OK

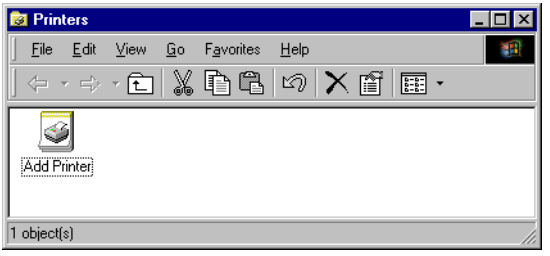
7. After rebooting your computer, add the Barricade print server to your system as described in the following section.

Configure the Print Server

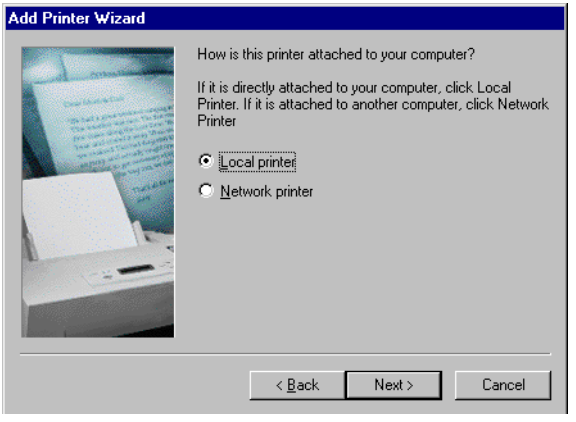
The Barricade's print server supports Microsoft Windows 95/98/Me/NT/2000/XP and Unix. If you are using Windows 95/98/Me/NT/2000/XP, first install the port monitor as described in the previous section before adding the Barricade's print server to your operating system.

Configure the Network Printer in Windows 95/98/Me/2000

1. On a Windows 95/98/Me/2000/XP platform, open the Printers window in the My Computer menu, and double-click the "Add Printer" icon.

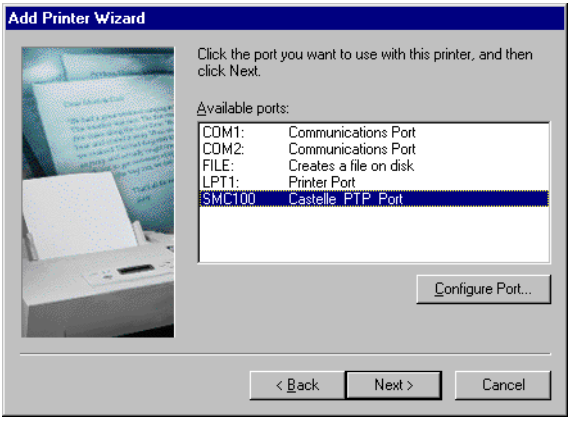


2. Follow the prompts to add a local printer to your system.

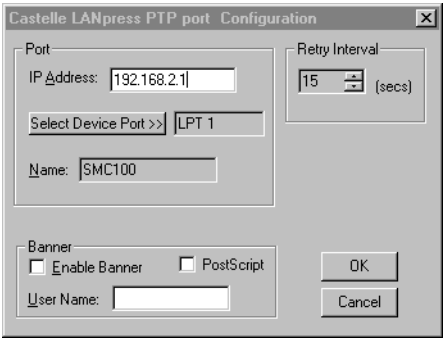

Add Printer Wizard
How is this printer attached to your computer?
If it is directly attached to your computer, click Local Printer. If it is attached to another computer, click Network Printer
Local printer
Network printer
< Back
Next >
Cancel

3. Specify the printer type attached to the Barricade.

4. Select the monitored port. The default port name is "SMC100." Click the "Configure Port" button.


Add Printer Wizard
Click the port you want to use with this printer, and then click Next.
Available ports:
COM1: Communications Port
COM2: Communications Port
FILE: Creates a file on disk
LPT1: Printer Port
SMC100 Castelle PTP Port
Configure Port...
< Back
Next >
Cancel

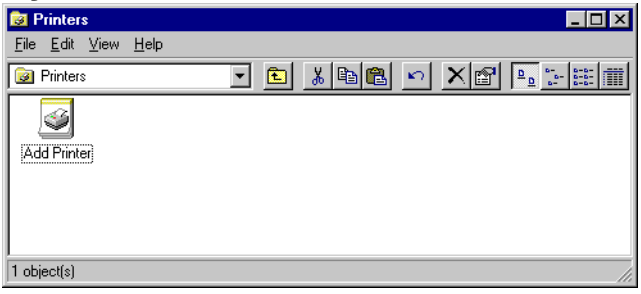
5. Enter the IP address of the Barricade and click "OK." Then click "Next" in the Add Printer Wizard dialog box.



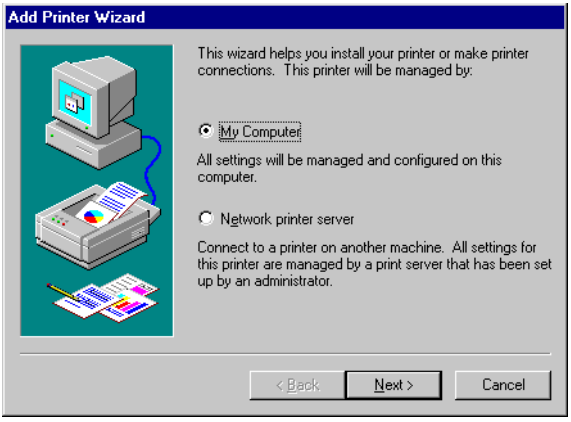
6. Continue following the prompts to complete the installation of the Barricade print server. The printer will now be added to your Printers menu.

Configure the Network Printer in Windows NT

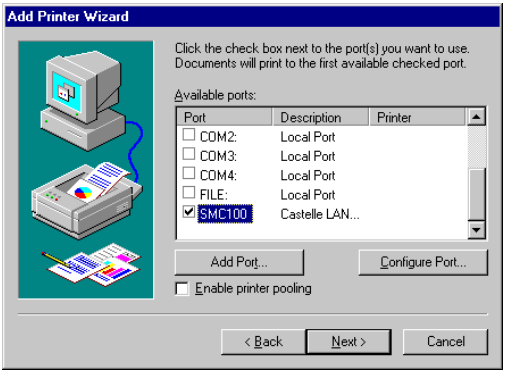
1. On a Windows NT platform, open the Printers window in the My Computer menu, and double-click the "Add Printer" icon.



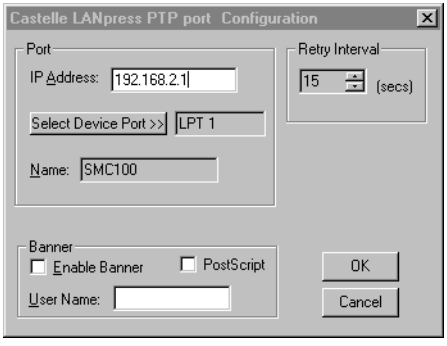
2. Follow the prompts to add a local printer to your system.


Add Printer Wizard
This wizard helps you install your printer or make printer connections. This printer will be managed by:
My Computer
All settings will be managed and configured on this computer.
Network printer server
Connect to a printer on another machine. All settings for this printer are managed by a print server that has been set up by an administrator.
< Back
Next >
Cancel

3. Select the monitored port. The default port name is "SMC100." Then click the "Configure Port" button.



4. Enter the IP address of the Barricade and click "OK." Click "Next" in the Add Printer Wizard dialog box.



5. Specify the printer type attached to the Barricade.

6. Continue following the prompts to complete the installation of the Barricade print server. The printer type you specified will now be added to your Printers menu.

Configure the Network Printer in Unix Systems

Follow the standard configuration procedure on your Unix platform to set up the Barricade print server. The printer name is "lpt1."

APPENDIX A
TROUBLESHOOTING

This section describes common problems you may encounter and possible solutions to them. The Barricade can be easily monitored through panel indicators to identify problems.

Troubleshooting Chart	
Symptom	**Action**
LED Indicators	
Power LED is Off	• Check connections between the Barricade, the external power supply, and the wall outlet. • If the power indicator does not turn on when the power cord is plugged in, you may have a problem with the power outlet, power cord, or external power supply. However, if the unit powers off after running for a while, check for loose power connections, power losses, or surges at the power outlet. If you still cannot isolate the problem, then the external power supply may be defective. In this case, contact Technical Support for assistance.

Troubleshooting Chart	
Symptom	**Action**
LED Indicators	
Link LED is Off	• Verify that the Barricade and attached device are powered on. • Be sure the cable is plugged into both the Barricade and the corresponding device. • Verify that the proper cable type is used and that its length does not exceed the specified limits. • Be sure that the network interface on the attached device is configured for the proper communication speed and duplex mode. • Check the adapter on the attached device and cable connections for possible defects. Replace any defective adapter or cable if necessary.
Network Connection Problems	
Cannot Ping the Barricade from the attached LAN, or the Barricade cannot Ping any device on the attached LAN	• Verify that the IP addresses are properly configured. For most applications, you should use the Barricade's DHCP function to dynamically assign IP addresses to hosts on the attached LAN. However, if you manually configure IP addresses on the LAN, verify that the same network address (network component of the IP address) and subnet mask are used for both the Barricade and any attached LAN devices. • Be sure the device you want to Ping (or from which you are Pinging) has been configured for TCP/IP.

Troubleshooting Chart	
Symptom	**Action**
Management Problems	
Cannot connect using the Web browser	• Be sure to have configured the Barricade with a valid IP address, subnet mask, and default gateway. • Check that you have a valid network connection to the Barricade and that the port you are using has not been disabled. • Check the network cabling between the management station and the Barricade.
Forgot or lost the password	• Press the Reset button on the rear panel (holding it down for at least five seconds) to restore the factory defaults.

APPENDIX B
CABLES

Ethernet Cable

Caution: Do not plug a phone jack connector into an RJ-45 port. For Ethernet connections, use only twisted-pair cables with RJ-45 connectors that conform to FCC standards.

Specifications

Cable Types and Specifications			
Cable	**Type**	**Max. Length**	**Connector**
10BASE-T	Cat. 3, 4, 5 100-ohm UTP	100 m (328 ft)	RJ-45
100BASE-TX	Cat. 5 100-ohm UTP	100 m (328 ft)	RJ-45

Wiring Conventions

For Ethernet connections, a twisted-pair cable must have two pairs of wires. Each wire pair is identified by two different colors. For example, one wire might be red and the other, red with white stripes. Also, an RJ-45 connector must be attached to both ends of the cable.

Each wire pair must be attached to the RJ-45 connectors in a specific orientation. The following figure illustrates how the pins on an Ethernet RJ-45 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.

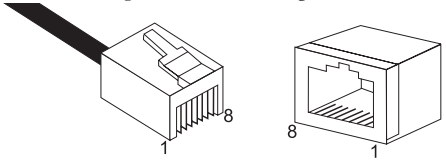


Figure B-1. RJ-45 Ethernet Connector Pin Numbers

RJ-45 Port Ethernet Connection

Use the straight-through CAT -5 Ethernet cable provided in the package to connect the Barricade to your PC. When connecting to other network devices such as an Ethernet switch, use the cable type shown in the following table.

Attached Device Port Type	Connecting Cable Type
MDI-X	Straight-through
MDI	Crossover

Pin Assignments

With 10BASE-T/100BASE-TX cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 for receiving data.

RJ-45 Pin Assignments	
Pin Number	Assignment*
1	Tx+
2	Tx-
3	Rx+
6	Rx-

* The "+" and "-" signs represent the polarity of the wires that make up each wire pair.

Straight-Through Wiring

If the port on the attached device has internal crossover wiring (MDI-X), then use straight-through cable.

Straight-Through Cable Pin Assignments	
End 1	End 2
1 (Tx+)	1 (Tx+)
2 (Tx-)	2 (Tx-)
3 (Rx+)	3 (Rx+)
6 (Rx-)	6 (Rx-)

Crossover Wiring

If the port on the attached device has straight-through wiring (MDI), use crossover cable.

Crossover Cable Pin Assignments	
End 1	End 2
1 (Tx+)	3 (Rx+)
2 (Tx-)	6 (Rx-)
3 (Rx+)	1 (Tx+)
6 (Rx-)	2 (Tx-)

ADSL Cable Connection

Use standard telephone cable to connect the RJ-11 telephone wall outlet to the RJ-11 ADSL port on the ADSL Router.

Caution: Do not plug a phone jack connector into an RJ-45 port.

Specifications

Cable Types and Specifications		
Cable	**Type**	**Connector**
ADSL Line	Standard Telephone Cable	RJ-11

Wiring Conventions

For ADSL connections, a cable requires one pair of wires. Each wire is identified by different colors. For example, one wire might be red and the other, red with white stripes. Also, an RJ-11 connector must be attached to both ends of the cable.

Each wire pair must be attached to the RJ-11 connectors in a specific orientation. The following figure illustrates how the pins on the RJ-11 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.

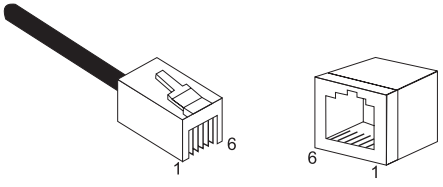
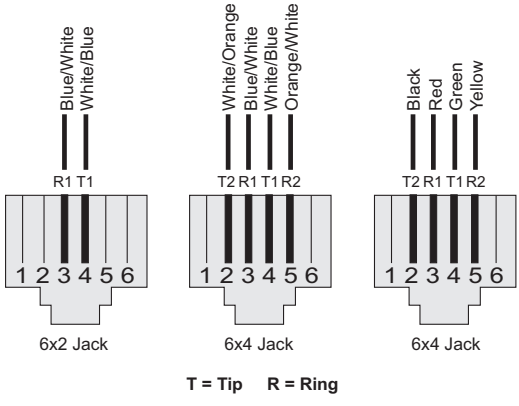


Figure B-2. RJ-11 Connector Pin Numbers



Pin	Signal Name	Wire Color
1	*Not used*	
2	Line 2 Tip	Black or White/ Orange
3	Line 1 Ring	Red or Blue/ White
4	Line 1 Tip	Green or White/Blue
5	Line 2 Ring	Yellow or Orange/ White
6	*Not used*	

Figure B-3. RJ-11 Pinouts

APPENDIX C
SPECIFICATIONS

Standards Compliance

CE Mark

Emissions

- FCC Class B
- VCCI Class B
- Industry Canada Class B
- EN55022 (CISPR 22) Class B
- C-Tick - AS/NZS 3548 (1995) Class B

Immunity

- EN 61000-3-2/3
- EN 61000-4-2/3/4/5/6/8/11

Safety

- UL 1950
- EN60950 (TÜV)
- CSA 22.2 No. 950

IEEE 802.3 10 BASE-T Ethernet

IEEE 802.3u 100 BASE-TX Fast Ethernet

Modem Standards

- ITU G.992.1 (G.dmt)
- ITU G.992.2 (G.Lite)
- ITU G.994.1 (G.handshake)
- ITU T.413 issue 2 - ADSL full rate

LAN Interface

4 RJ-45 10 BASE-T/100 BASE-TX ports

Auto-negotiates the connection speed to 10 Mbps Ethernet or 100 Mbps Fast Ethernet, and the transmission mode to half-duplex or full-duplex.

WAN Interface
1 ADSL RJ-11 port

Indicator Panel
Power, Ethernet, ADSL Syn, ADSL Data

Dimensions
220 x 132.8 x 30.5 mm

Weight
0.6 kg

Input Power
12 V 1 A

Power Consumption
12 Watts max.

Management
Web management

Advanced Features
Dynamic IP Address Configuration – DHCP, DNS
Firewall – Client privileges, hacker prevention and logging, Stateful Packet Inspection
Virtual Private Network – PPTP, IPSec pass-through, VPN pass-through

Internet Standards
RFC 826 ARP, RFC 791 IP, RFC 792 ICMP, RFC 768 UDP, RFC 793 TCP, RFC 783 TFTP, RFC 1483 AAL5 Encapsulation, RFC 1661 PPP, RFC 1866 HTML, RFC 2068 HTTP, RFC 2364 PPP over ATM

Temperature
Operating 0 to 40°C
Storage -40 to 70°C

Humidity
5% to 95% (noncondensing)

Warranty
Limited Lifetime

LIMITED WARRANTY

SMC's Limited Warranty Statement

Limited Warranty Statement: SMC Networks Europe ("SMC") warrants its products to be free from defects in workmanship and materials, under normal use and service, for the applicable warranty term. All SMC products carry a standard 2 year limited warranty from the date of purchase from SMC or its Authorized Reseller. SMC may, at its own discretion, repair or replace any product not operating as warranted with a similar or functionally equivalent product, during the applicable warranty term. SMC will endeavour to repair or replace any product returned under warranty within 30 days of receipt of the product. As new technologies emerge, older technologies become obsolete and SMC will, at its discretion, replace an older product in its product line with one that incorporates these newer technologies

The standard limited warranty can be upgraded to a 5 year Limited Lifetime * warranty by registering new products within 30 days of purchase from SMC or its Authorized Reseller. Registration can be accomplished via the enclosed product registration card or online via the SMC web site. Failure to register will not affect the standard limited warranty. The Limited Lifetime warranty covers a product during the Life of that Product, which is defined as a period of 5 years from the date of purchase of the product from SMC or its authorized reseller.

All products that are replaced become the property of SMC. Replacement products may be either new or reconditioned. Any replaced or repaired product carries, either a 30-day limited warranty or the remainder of the initial warranty, whichever is longer. SMC is not responsible for any custom software or firmware, configuration information, or memory data of Customer contained in, stored on, or integrated with any products returned to SMC pursuant to any warranty. Products returned to SMC should have any customer-installed accessory or add-on components, such as expansion modules, removed prior to returning the product for replacement. SMC is not responsible for these items if they are returned with the product.

Customers must contact SMC for a Return Material Authorization number prior to returning any product to SMC. Proof of purchase may be required. Any product returned to SMC without a valid Return Material Authorization (RMA) number clearly marked on the outside of the package will be returned to customer at customer's expense. Customers are responsible for all shipping charges from their facility to SMC. SMC is responsible for return shipping charges from SMC to customer.

WARRANTIES EXCLUSIVE: IF A SMC PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT OF THE PRODUCT IN QUESTION, AT SMC'S OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SMC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. SMC SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), SHALL SMC BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF SMC OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME COUNTRIES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, WHICH MAY VARY FROM COUNTRY TO COUNTRY. NOTHING IN THIS WARRANTY SHALL BE TAKEN TO AFFECT YOUR STATUTORY RIGHTS.

* Under the limited lifetime warranty, internal and external power supplies, fans, and cables are covered by a standard one-year warranty from date of purchase.

Full Installation Manual
Full installation manuals are provided on the Installation CD-Rom. Manuals in other languages than those included on the CD-Rom are provided on www.smc-europe.com (section support).

Firmware and Drivers
For latest driver, technical information and bug-fixes please visit www.smc-europe.com (section support).

Contact SMC
Contact details for your relevant countries are available on www.smc-europe.com and www.smc.com.

Statement of Conditions
In line with our continued efforts to improve internal design, operational function, and/or reliability, SMC reserves the right to make changes to the product(s) described in this document without notice. SMC does not assume any liability that may occur due to the use or application of the product(s) described herein. In order to obtain the most accurate knowledge of installation, bug-fixes and other product related information we advise to visit the relevant product support page at www.smc-europe.com before you start installing the equipment. All information is subject to change without notice.

Limitation of Liability
In no event, whether based in contract or tort (including negligence), shall SMC be liable for incidental, consequential, indirect, special or punitive damages of any kind, or for loss of revenue, loss of business or other financial loss arising out of or in connection with the sale, installation, maintenance, use, performance, failure or interruption of its products, even if SMC or its authorized reseller has been adviced of the possiblity of such damages.

Copyright
Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

Trademarks
SMC is a registered trademark; and EZ Connect is a trademark of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders.